Enterprise Risk

Summer 2019 / www.enterpriseriskmag.com

The official magazine of the Institute of Risk Management

Weight of numbers: quantitative risk management focus / **Mental blocks:** the truth about cryptocurrency safety / **Cookie cutters:** getting ready for ePrivacy / **Changing the climate on risk:** addressing environmental threat

Securing a future: Nagumantry Roop Kumar on SBI Life's plans to deliver insurance to India's huge population

Enterprise Risk

Summer 2019

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

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

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

Institute of Risk Management
2nd Floor, Sackville House, 143-149
Fenchurch Street, London, EC3M 6BN
Tel: +44 (0)20 7709 9808
Fax: +44 (0)20 7709 0716
enquiries@theirm.org
www.theirm.org

Editorial

Working through change

There is something of a technology flavour to this issue. For the cover story, I spoke to Nagumantry Roop Kumar, who heads up risk at India's SBI Life Insurance. Today, only four in 100 Indians have insurance, and the business of the insurance salesperson knocking on doors in remote villages to sell contracts is time-consuming and – to be honest – fairly unrealistic.

While insurers have teamed up with banks to gain access to their customers, the best hope of revolutionising the market is via mobile phones – a mode of communication which has spread rapidly throughout the country. Roop Kumar has been working hard to transform the business to take advantage of this trend and manage sometimes complex and strange risks the enterprise faces – such as Deadman insurance. No spoilers here!

As if that were not enough, the regulatory landscape is also changing quickly in India with tighter data laws in the offing. While UK and European risk managers will have had enough of hearing about the General Data Protection Regulation (GDPR), which tightens personal privacy laws, we take a look at its lesser-known cousin, the forthcoming ePrivacy Regulation. It brings GDPR to the world of cookies and mobile technology, even if the finer details have yet to be decided.

> **Global trends are both changing the technologies businesses use and the tools and techniques risk managers need to adopt to help their organisations take advantage of the changing risk landscape**

These global trends are both changing the technologies businesses use and the tools and techniques risk managers need to adopt to help their organisations take advantage of the changing risk landscape. We are hoping to explore these issues later in the year with a member survey on technology software. Keep an eye out for the questionnaire when it arrives in your inbox.

Finally, The Institute of Operational Risk (IOR) will be joining the IRM group following a vote by its members at their annual general meeting this May. While the details of the future strategy are to be decided, in the collaboration IRM will provide full support for the promotion of the IOR Certificate in Operational Risk Management. This will ultimately become part of the IRM's global portfolio of qualifications, complementing the International Certificate and Diploma in ERM, the International Certificate in Financial Services, and the new Digital Risk Management Certificate.

In a world driven by fast-changing trends in technology, demographic growth and other uncertainties, greater collaboration among risk professionals is essential.

Arthur Piper
Editor

Contents

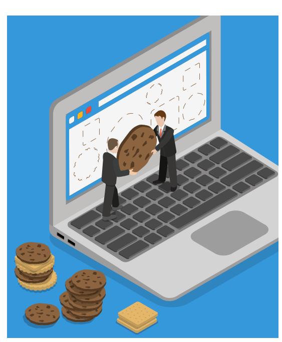
10

FEATURES

REGULARS

16

20



24

28

Joining forces

The Institute of Operational Risk is joining the IRM

IRM was delighted to announce in May that the Institute of Operational Risk (IOR) will be joining the IRM group. This came following a vote at the IOR Annual General Meeting held on Wednesday, May 22, in London.

As our members – both existing and new – are probably aware, IRM's prime objective is to provide education and training for the global risk management community, and to support the profession with cutting-edge thought leadership. The IOR has the same and complementary purpose focused on operational risk. Both organisations recognise that strong benefits and synergies can be achieved by coming together.

IRM will in particular provide full support for the promotion of the IOR Certificate in Operational Risk Management. This will ultimately become part of the IRM's global portfolio of qualifications, complementing the International Certificate and Diploma in ERM, and the new Digital Risk Management Certificate.

As part of our agreement, IRM will be funding a major joint research project to advance thinking in operational risk management and contribute to further qualifications development. IRM and IOR are jointly committed to advancing the practice of operational risk management as we enter the Fourth Industrial Revolution.

The development of a global network of risk practitioners and professionals delivering value and service at a local and regional level is a key strategy of both the IRM and IOR. The chapters and groups of the two organisations will co-operate at a regional level to provide global support for members and the wider risk management community.

The IOR brand will be retained and will continue to represent excellence in the practice and profession of operational risk management.

In fact, the IRM has had a long and productive association with the IOR. We have built our partnership on the common ground between us and the joint interest we have in providing excellent education and training to the wider global risk community.

Our groups and chapters complement one another. We believe it is in the interest of both institutes to further deepen and extend our strategic relationship. The exact form of the future strategy is currently under discussion, but we are positive that whatever the direction taken the outcome will be in the best interests of the risk management profession.

> **The development of a global network of risk practitioners and professionals delivering value and service at a local and regional level is a key strategy of both the IRM and IOR**

George Clark, FIOR, chair of the IOR, agrees that this is a wonderful opportunity for both the IOR and IRM to make a difference to the conversation on the future of operational risk management and practice. "We know that we have much in common and this new relationship leverages both greater scale and complementary thought leadership and competencies. I am certain our members and wider communities will benefit greatly," he said.

Socrates Coudounaris CFIRM **is chairman of the IRM.**

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

Legal profession highlights extent of workplace bullying and harassment

Bullying in legal workplaces affects

1 in 2 female respondents

1 in 3 male respondents

Sexual harassment affects

1 in 3 female respondents

1 in 14 male respondents

YET ONLY

53% of firms had policies to address bullying and sexual harassment

22% of firms undertook training

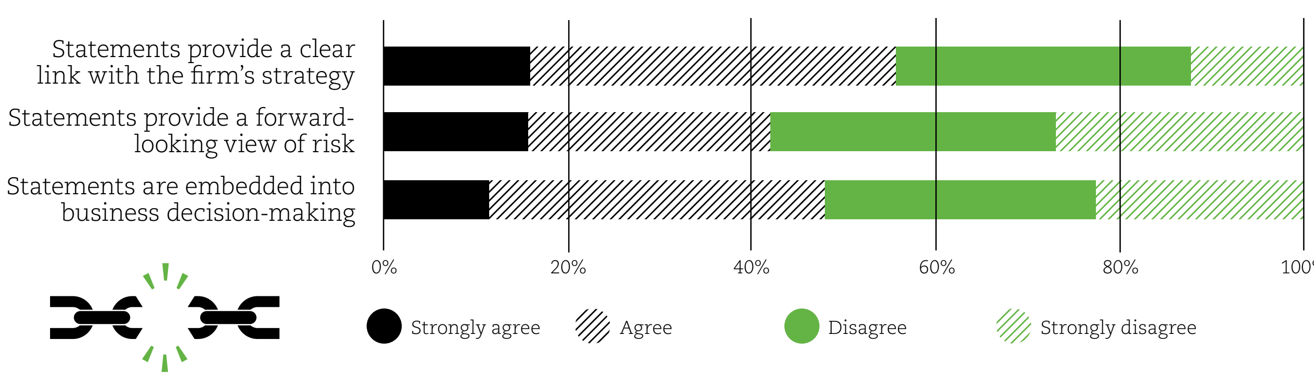
Targets leaving unsupportive workplaces because of:

65% Bullying

37% Sexual harassment

Source: Us too? Bullying and sexual harassment in the legal profession, International Bar Association

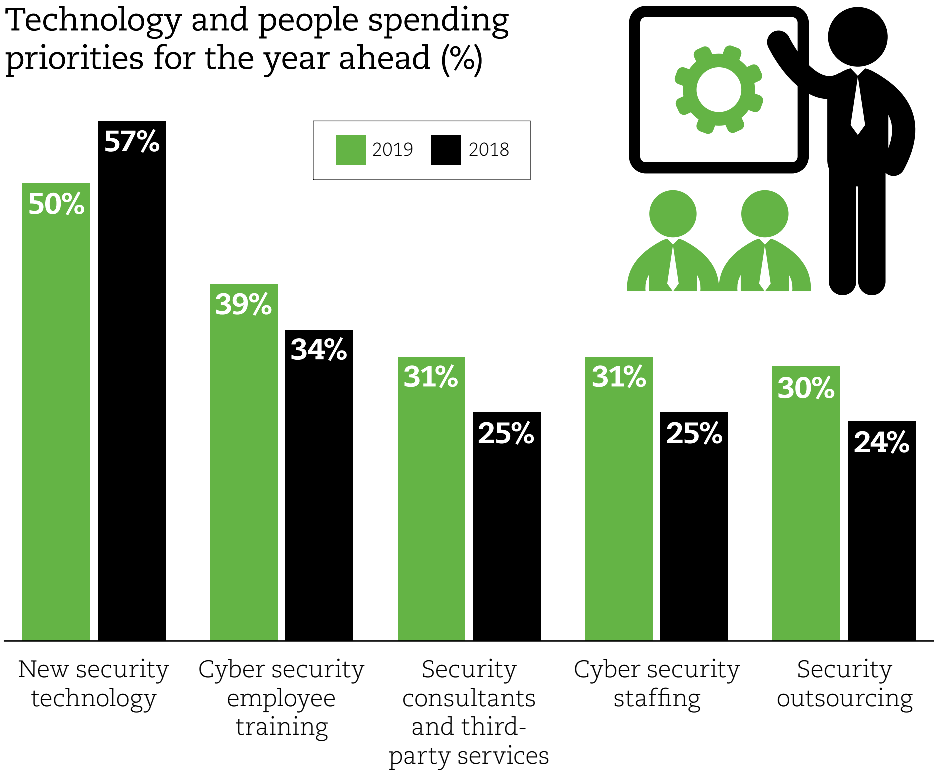
Risk appetite statements failing to link with business practices



Source: Baringa partners' operational risk report, Baringa partners

Businesses increase cyber defence spending on staff and training

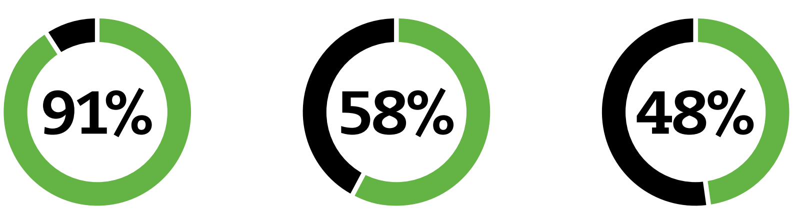
Technology and people spending priorities for the year ahead (%)



Source: Hiscox Cyber Readiness Report 2019, Hiscox

Employees lax on data transfers

A poll of over 300 employees across a wide range of sectors showed a careless attitude to using USB drives at work to transfer data



Those saying encrypted USB drives should be mandatory

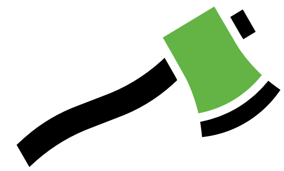
Those saying they regularly use unencrypted USB drives

Those who do not notify their organisations after losing a USB drive

Source: The state of USB data protection 2019: Employee spotlight, Apricorn

Risky vendors face the axe

Over half of businesses say they are likely to exit or de-risk their vendor relationships



41%

It's become imperative from a risk and regulatory standpoint to also assess our vendors' subcontractors

33%

The cost associated to assess our vendors properly is becoming too high

27%

We lack the internal support and/or skills for the required sophisticated forensic control testing of our vendors

24%

We do not have the right technologies in place to assess vendor risk properly

19%

We will not receive sufficient internal support to "de-risk" our vendor relationships

Source: 2019 vendor risk management benchmark survey: running hard to stay in place, Shared Assessments Program and Protiviti

Securing a future

The head of risk at SBI Life Insurance, Nagumantry Roop Kumar, explains why delivering life insurance to India's huge population is a work in progress

BY ARTHUR PIPER

The Indian insurance sector is growing at an impressive rate. The government's policy to insure the uninsured has helped boost the number and types of policies on offer – with gross premiums reaching about $71 billion in 2018, according to government figures. Pundits expect the industry to carry on expanding rapidly because of a growing economy, continuing changes in regulation and the fact that fewer than four in 100 Indians have any sort of insurance.

On October 3, 2017, one of the major players in the Indian life insurance industry, SBI Life Insurance, listed on the Bombay Stock Exchange and National Stock Exchange of India. SBI Life Insurance is a joint venture between the State Bank of India and BNP Paribas Cardif – and as at March 31, 2019, it had assets under management of about $20.7 billion, ranking second in the country for new business premium among private players. It is hoping to build on its significant share in the market over the coming years.

But the industry faces stiff challenges, according to Nagumantry Roop Kumar, executive vice president and chief of risk, information and cyber security management at SBI Life, who took the reins as the organisation's head of risk back in April 2014. These are partly due to the sector's

> **Low-cost products which can be priced to give even a marginal profit, multiplied into huge volumes that is the population of India, represent a huge opportunity for insurers**

history. The life insurance industry nationalised in 1956, with the state-owned Life Insurance Corporation of India existing as a monopoly player in the sector. The industry opened up to private companies in the late 1990s. While there are around 23 life and 28 general private insurers in the sector, product distribution and innovation still need to be improved and fine-tuned to meet the needs of the Indian population.

"Selling market segment-oriented products, and focusing on customer aspiration and satisfaction is a challenge," Roop Kumar says. For example, in the past, state-owned insurers relied exclusively on using tied agents to sell their products. This is still an important channel for selling insurance, but it is time-consuming and expensive. Insurance agents need recruiting and once trained often need to meet with clients more than once to secure a sale. Outside of the large cities, rural travel distances can be relatively long, which adds to an already burdensome process.

Changing channels

Bank assurance has recently taken over as the pre-eminent sales channel for Indian insurers. It enables SBI Life and others to sell insurance through their banking partners. Those banks have a captive client base, which they leverage, by cross selling and upselling insurance products in addition to their core services.

"Generally, most of the people with a bank account in India are middle class and upper-middle class, and banks are able to get a good healthy premium from them," Roop Kumar explains. But online sales are also picking up rapidly and insurers need to innovate if they are to significantly improve the country's low level of insurance penetration.

Prospects are promising. Mobile phone use is widespread. Online selling over such devices will better serve a mostly rural population. Because the Indian economy has been growing steadily at around 7 per cent for the last 15 years, India has a rising middle class with higher aspirational levels. This segment of the population is no longer just confined to the big cities alone – and they have disposable income. Reaching those people is the core aim for insurers, and mobile devices are key to unlocking the market.

"To approach them, we should move from a distributor-driven process into a technology-driven business model," Roop Kumar says. "That, again, is going to happen because of the opportunities created by smartphones and access to data

> I try to make it as simple as possible – and make people feel that being aware of risk actually secures them

that people have." Data in India is among the cheapest in the world. It is still relatively less regulated compared with jurisdictions such as Europe; however, stiffer privacy regulations similar to the General Data Protection Regulation (GDPR) are in the offing.

For this strategy to pay off, insurers need to innovate their products. At the bottom end of the pyramid, the government of India is providing insurance schemes at a very low cost, such as term insurance and medical insurance and affordable pension schemes. Roop Kumar says these initiatives are beginning to pay dividends as people become more aware of the potential benefits of insurance.

"Low-cost products which can be priced to give even a marginal profit, multiplied into huge volumes that is the population of India, represent a huge opportunity for insurers," he says. Companies are testing demand, for instance, by creating term products without heavy underwriting, processing and distribution costs – but he says they have not yet been developed successfully enough to take off in a big way.

"Products are being tested and put in the market and then being refined," he says. "Over the next two to three years, to a maximum of five years, you will see a sea-change in the way insurance is being bought and sold in the country."

Deadman insurance

The insurance industry faces other challenges, not least from the widespread and often imaginative fraudulent schemes that thrive in the region. "We have a strange phenomenon called Deadman insurance – the person is already dead, but the proposal comes in fully manufactured," says Roop Kumar. "Then we get a claim within a year or two. This has become very rampant and fraudulent insurance claims are one of the biggest challenges insurers are facing."

He says the practice has become so common that insurers are seeing underwriting profits being affected, company costs rising and profit margins slimming.

"When we started getting a lot of incidents of very early death claims and fraudulent claims, we set up a risk analytics team within

risk management since he took up the post five years ago in what was then an unlisted joint enterprise. SBI Life was the first life insurance company in India to be compliant with the ISO 31000 ERM Standard, a process that he oversaw. Last year, it added COSO 2017 to its methodologies to help assess the maturity of the business' ERM practices, and Roop Kumar's team is busy making further changes to the risk management processes.

His remit is wide and takes in strategic risk assessment, business continuity planning and governance, all of which have processes that are strongly documented. In addition to the usual operational, market, hazard and product risks you would expect such a function to oversee, he is also responsible for business continuity, information security, data protection, fraud monitoring and business analytics. Each of the latter are distinct specialities in SBI Life with their own heads of function reporting to Roop Kumar. He reports to the company's risk management committee on all of these issues.

Five years ago, when he started out in the business, he admits that the industry was not so conscious of risk. Now he says he would describe risk awareness among managers as a significant trait – particularly since he ran a risk culture programme in the lead-up to SBI Life's public listing.

"We wanted to build up the risk awareness level from the top management right to the last person," he explains. "Every employee in the company has a fairly good idea about risk, has the responsibility to manage risk and the tools to understand risk. It is now part of the daily work culture."

This has taken a lot of work and training and is an important, ongoing part of Roop Kumar's portfolio. The regional risk officers, for example, have specially designed risk guidelines and visit their branch offices to conduct training sessions. They also teach staff how to handle risk management tools and how to understand risk.

It is not all one-way communication though. During risk management week, the team conducts a lot of quizzes and competitions. Recently, they held a poster competition – the best risk slogans were made by employees from the branch offices. "The slogans came from them, not us," he says proudly. There is also online training.

In fact, staff are marked on their understanding of risk in a way that feeds into their key performance indicators. "They are very proactive and aspire to get good marks in it," he says, "but I wouldn't be able to do all of these things without the support of the top management downwards."

the risk function," he says. They examined very early death claims in the company over the previous five years – looking for the triggers in the proposal forms that indicated potential fraud. They also factored in the quality of business from each distributor and fraud incidents experienced by other companies. The result was an in-house program called Risk Score, in which they partnered with the underwriters. In addition, the company created a fraudulent risk claim verification program, which is used to investigate potential fraud, even post-issuance of a policy.

"There are external fraud agencies who investigate, but the volumes are very high and, keeping in mind the cost of investigation, we need to point them towards some specific policies, proposals and geographies which look extremely risky," he says. "We bring it down to something like 3 per cent of policies that we have sourced and then give it to the investigating agencies for verification."

Risk focus

Roop Kumar has been working hard to develop this level of sophistication in

Top to bottom

SBI Life has a dedicated central ERM team, which is further supported by operational regions in the country. He encourages his risk managers to seek certification, such as those offered by IRM, and looks initially for staff with strong analytical skills. But networking skills are paramount – without the ability to get buy-in from top management and communicate effectively with the business, risk management becomes relegated to a compliance role, he says.

The risk team broadly follows ISO 31000 and the COSO 2017 framework. What that means in practice is that risk awareness is ingrained throughout the entire organisation, down to what Roop Kumar calls "the last person".

"I have a risk mantra, just like all Indians have mantras," he says, laughing. "Everywhere I go and whatever I do I propagate this mantra through my communications and everything – 'ERM means everyone is a risk manager'. To support it, we have a saying in the company which is put up everywhere in every office – 'be risk aware, be data aware and be secure'."

Data

Recently, Roop Kumar has been focusing on data protection and data leakage. In India, current data protection laws have few teeth, so data leakage is rampant. "The need to do more to raise

> **"ERM means, everyone is a risk manager**

consciousness about how to secure data and not to be frivolous with it has become a huge concern," he says. "To build processes around data is a challenge that I have."

To help with the issue, the business re-examined the processes to map data flows across the entire company. All data from unprotected formats goes into a data flow analysis, and the risk team consults with individual departments to look at safer ways to control and monitor it.

He has also put in place a data leakage prevention initiative. "Under this project, all the data that is flowing within the organisation and going out of the organisation is being monitored – and we are putting in rules to manage that data flow as we get a better understanding of it," he says.

In tandem with this, the company is strengthening its mobile device data management. SBI Life has over 100,000 distribution staff, many of whom are part-time. They are based everywhere from cities to deep rural areas, and many have started working extensively on smartphones and tablets, creating large flows of data to and from the company's systems. The risk team has put in place a mobile device management program to control this data flow through a secure channel.

As well as there being a solid business reason for taking such measures, there are upcoming regulatory reasons too. Roop Kumar believes that a more powerful data protection act could come into force soon after the Indian parliamentary elections, which had just ended at the time of writing. It will be a big challenge for the risk team because they will need to examine all the contracts where the company handles the data, plug all data flows that could lead to data leakage and potentially modify a lot of systems and processes to comply with the law while simultaneously bringing up awareness levels.

"People may actually be moving data around randomly without understanding the implications of what they are doing," he says. With over 15,000 employees spread over 909 offices (as at April 2019), awareness training alone will require a mammoth effort. "It is going to be a journey and we have already started in anticipation of the upcoming act, otherwise we would not be able to catch up with it," he says.

Image credit: sladkozaponi / Shutterstock.com

Above: Fewer than four in 100 Indians have insurance

Variety

Roop Kumar enjoys the variety that his role provides. He spent 32 years heading business-critical functions such as sales, marketing, operations, legal, IT and customer services before opting for his current role.

"I have a good understanding of how risks originate, how the data flows and how the risks happen in the company," he says. "I use this experience to design and develop effective risk-based solutions – and deliver them to the last person. I try to make it as simple as possible – and make them feel that being aware of risk actually secures them; I sincerely believe in that."

While he admits that there is pressure to demonstrate results to the business, there seems to be an almost moral dimension to his view of the importance of risk. He speaks of personal data as being as important as their other assets – houses, cars or jewellery – which gives the company an ethical responsibility to protect those people from harm. "Wearing my business continuity hat," he says at another point during the interview, "I see a lot of people who are dispossessed and companies that are struggling, so coming up with solutions for that are important." That is one of the reasons he sees his current role as a kind of capstone to his career. It helps him bring all his knowledge and skills together for the benefit of others.

"I see a lot of people who are dispossessed and companies that are struggling, so coming up with solutions for that are important

Institute of Risk Management

Risk Management Training

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

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

We offer CPD and accreditation.

> *"IRM is not just a training institution, it's a community that shares knowledge, experience and networking opportunities which has contributed to the furthering of my career."*
>
> **Richard Hawkins, CIRM**
> **Business Analyst**
> **Rimelo Consulting**

Training courses include:

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

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

irm

Weight of numbers

Risk managers looking to better understand and use quantitative risk analysis can take advantage of a new IRM training initiative with partnering organisation Real Options Valuation

BY PROFESSOR DR JOHNATHAN MUN

Businesses have been dealing with risk since the beginning of the history of commerce. In most cases, managers have looked at the risks of a particular project, acknowledged their existence and moved on. Little quantification was performed in the past. In fact, most decision-makers look only to *single-point estimates* of a project's profitability, cost, time to completion, revenues and so on.

Risk should be an important part of the decision-making process; without an assessment of risk, bad decisions may be made. For instance, if projects are chosen based simply on an evaluation of returns, then clearly the highest-return project will be chosen over lower-return projects. In financial theory, projects with higher returns will, in most cases, bear higher risks. Therefore, instead of relying purely on bottom-line profits, a project should be evaluated based on its risks as well as its returns.

Instead of relying purely on bottom-line profits, a project should be evaluated based on its risks as well as its returns

IRM has teamed up with Real Options Valuation, Inc., a software, training and consulting firm located in Silicon Valley, California, to introduce and train analysts and decision-makers in the *Integrated Risk Management* framework. This framework comprises eight distinct phases of a successful and comprehensive risk analysis implementation, starting from a qualitative management screening process proceeding to quantitative risk-based

> Often the most valuable insight is created as decision-makers frame the complete problem to be resolved

decision modelling and, finally, to creating clear actionable intelligence and concise reports for management.

The patented process was developed by the author based on hundreds of previously successful implementations of risk analysis, stochastic forecasting, real options, valuation and optimisation projects both in the consulting arena and in industry-specific problems. These phases can be performed either in isolation or together in sequence for a more robust integrated analysis.

This article is only meant to be a high-level introduction to what can be deemed as a very powerful and insightful risk-based decision methodology. The methodology can be applied to any industry, across different aspects of a project or portfolio of programmes, using any financial or nonfinancial critical success factors and indicators. The accompanying graphic shows the Integrated Risk Management process up close. Briefly, we can separate the process into eight simple steps.

Qualitative management screening

Qualitative management screening is the first step in the Integrated Risk Management process. Decision-makers have to decide which projects, assets, initiatives or strategies are viable for further analysis, in accordance with the organisation's mission, vision, goal or overall business strategy, which may include strategies and tactics, competitive advantage, business development and technical, acquisition, growth, synergistic or globalisation issues. That is, the initial list of projects should be qualified in terms of meeting the decision-maker's agenda. Often the most valuable insight is created as decision-makers frame the complete problem to be resolved. This is where the various qualitative risks to the organisation are identified.

Forecast prediction modelling

The future is then forecasted using time-series analysis, stochastic forecasting or multivariate econometric/regression analyses if historical or comparable data exist. Otherwise, other qualitative forecasting methods may be used (subjective guesses, growth rate assumptions, expert opinions, Delphi method and so forth). These forecasts will be subjected to quantitative Monte Carlo risk-based simulations, such that probability distributions of the future are quantified.

Base-case static models

For each project that passes the initial qualitative screens, a quantitative model is created. This model serves as the base-case analysis – for example, net present value (NPV), return on investment (ROI), cost, schedule and so on – for each project, using the previously forecasted values. As an example, NPV is calculated using the traditional approach applying the forecasted revenues and costs and discounting the net of these revenues and costs at an appropriate risk-adjusted rate. ROI and other metrics are generated as required. Other quantitative models such as schedule-cost, enterprise risk, mergers and acquisition, and so forth can also be created in this step.

Dynamic Monte Carlo risk-based simulation

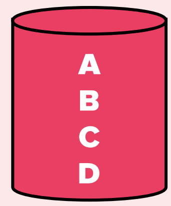
The previous static cash flow models produce only a single-point estimate result, and there is often

> Just because risk has been quantified to be such and such using Monte Carlo simulation, so what and what do we do about it?

INTEGRATED RISK MANAGEMENT PROCESS

RISK IDENTIFICATION

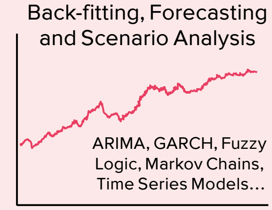
1 Qualitative Management Screening



Start with a list of projects or strategies to be evaluated that have already been through qualitative screening...

RISK PREDICTION

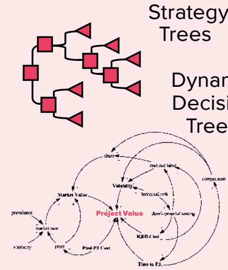
2 Forecast Prediction Modeling



...with the assistance of forecasting algorithms, future outcomes can be predicted...

RISK MITIGATION

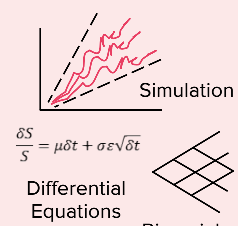
5 Real Options Problem Framing



...strategic real options are framed to hedge and mitigate downside risks and take advantage of upside potential...

RISK HEDGING

6 Real Options Valuation and Modeling



...the real options are valued using binomial lattices and closed-form partial-differential models with simulation...

Source: *Professor Johnathan Mun*

little confidence in its accuracy given that future events that affect forecast cash flows are highly uncertain. To better estimate the actual value of a particular project, Monte Carlo risk-based simulation should be employed next.

Usually, a sensitivity analysis is first performed on the model. For example, by setting the NPV, cost, schedule or ROI as the resulting variable, we can change each of its precedent variables and note the change in the resulting variable. Precedent variables include revenues, costs, tax rates, discount rates, capital expenditures, depreciation and so forth, which ultimately flow through the model to affect the NPV or ROI figure. By tracing back all these precedent variables, we can change each one by a preset amount and see the effect on the resulting NPV.

A graphical representation can then be created, which is commonly called a tornado chart because of its shape, where the most sensitive, precedent variables are listed first, in descending order of magnitude. Armed with this information, the analyst can then decide which key variables are highly uncertain in the future and which are deterministic.

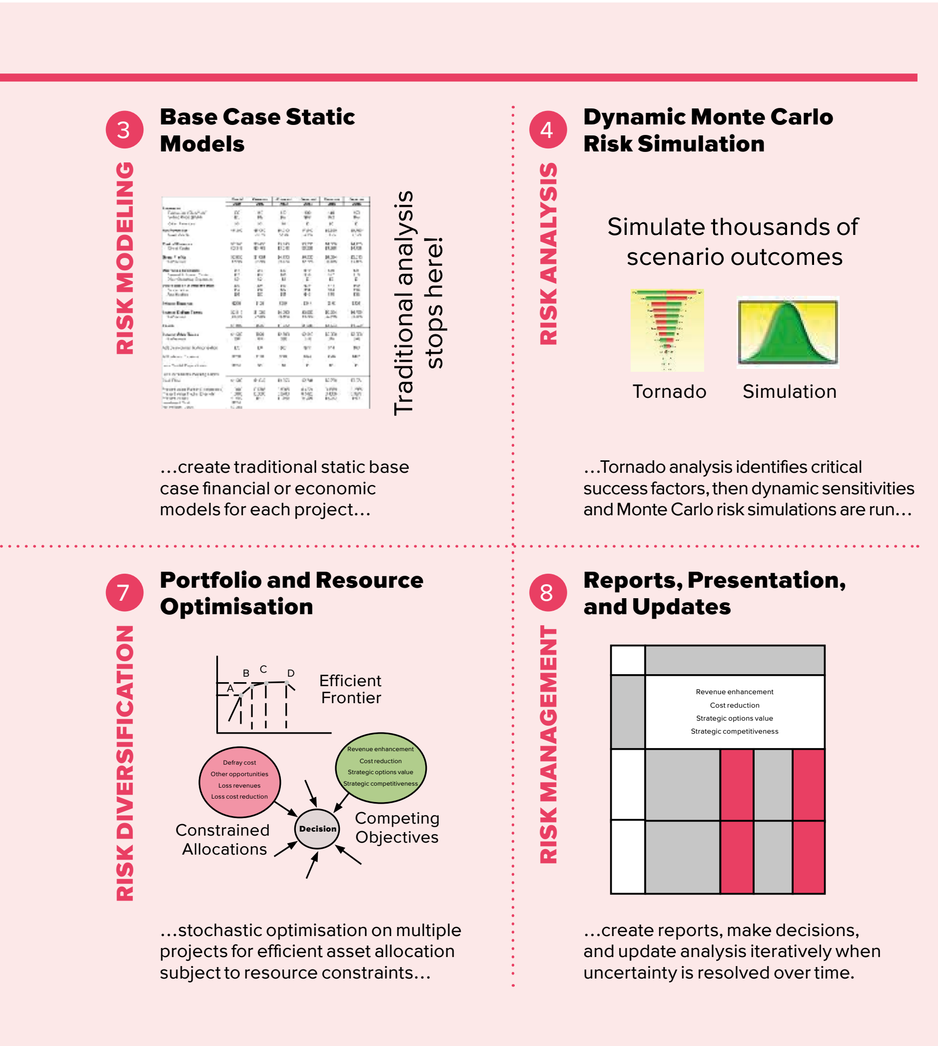
The uncertain key variables that drive the resulting variable of interest and, hence, the decision are called critical success drivers. These critical success drivers are prime candidates for Monte Carlo risk-based simulation. Because some of these critical success drivers may be correlated, a correlated and multidimensional Monte Carlo simulation may be required. Typically, these correlations can be obtained through historical data. Running correlated simulations provides a much closer approximation to the variables' real-life behaviours.

Real options problem framing

The question now is that after quantifying risks in the previous step, what next? The risk information obtained somehow needs to be converted into *actionable intelligence*. Just because risk has been quantified to be such and such using Monte Carlo simulation, so what and what do we do about it? The answer is to use real options analysis to hedge the downside risks, to value these risks and to position yourself to take advantage of the upside opportunities.

The first step in real options is to frame the project's strategic implementation pathways. Based on the overall problem identification occurring during the initial qualitative management screening process, certain strategic options or alternate investment pathways would have become apparent for each particular project. The strategic options may include, among other things, the option to expand, contract, abandon, switch, choose and so forth. Based on the identification of strategic options that exist for each project, or at each stage of the project, the analyst can then choose from a list of options to analyse in more detail.

Real options are added to the projects to hedge downside risks and to take advantage of upside swings. In this phase, complex systems modelling, system dynamics and game theory can also be applied. That is, the model can be set up as a system of multiple links or nested options, where one option is linked to another in unison – for example, complex simultaneous and sequential compound options. And the ramifications of competitors' actions can be included in the



model – for instance strategic, competitive games played in an oligopoly situation, where your opponent takes very different actions depending on the actions that you take, generating multiple potential scenarios and payoffs.

Real options valuation and modelling

Through the use of Monte Carlo simulation, the resulting stochastic model will have a probabilistic distribution of values. Thus, simulation models, analyses and quantifies the various risks and uncertainties of each project in that it results in a distribution of the NPVs and the project's volatility. In real options, we assume that the underlying variable is the future profitability of the project, which is the future cash flow series. An implied volatility of the future free cash flow or underlying variable can be calculated through the results of a Monte Carlo risk-based simulation previously performed. Using these inputs, quantitative real options models can be run to obtain the project's total strategic option values and to identify the best pathway forward for the project.

Portfolio and resource optimisation

Portfolio optimisation is an optional step in the analysis. If the analysis is performed on multiple projects, decision-makers should view the results as a portfolio of rolled-up projects. Viewing them individually will not present the true picture. As organisations do not only have single projects, portfolio optimisation is crucial. Given that certain projects

> **"** As organisations do not only have single projects, portfolio optimisation is crucial

are related to others, there are opportunities for hedging and diversifying risks through a portfolio. Because firms have limited budgets, time and other resource constraints, while at the same time having requirements for certain overall levels of returns, risk tolerances and so forth, portfolio optimisation takes into account all these factors to create an optimal portfolio mix. The analysis will provide the optimal allocation of investments across multiple projects. That is, given a set budget and resource constraints, we can quantitatively determine which projects should be selected in the portfolio.

Reports, presentation and updates

The results can then be presented as actionable intelligence to decision-makers, with the caveat that as things change over the course of time, actions and events, the analyses will need to be revisited and updated as required. After all, good managers should continually manage their projects and portfolios.

Professor Dr Johnathan Mun, PhD, MBA, MS, BS, CQRM, FRM, MIFC, is CEO of Real Options Valuation, Inc., and chairman of the International Institute of Professional Education and Research (IIPER). He is a professor at various universities globally and has developed more than 20 software applications in risk, predictive forecasting and quantitative decision analytics; he holds 11 patents and 10 patents pending; and he has authored over 24 books. His software, books and analytics are used by multinationals as well as taught at universities worldwide. Contact: jcmun@realoptionsvaluation.com

Mental blocks

Blockchain technology presents users with enhanced security and efficiency, but it is not without its challenges – including overcoming the ingrained habits of its users

BY ALEXANDER LARSEN AND FAISAL ALNAHDY

The last couple of years has seen a real buzz around a new technology called blockchain, which in essence is just a decentralised public database (the chain) of digital information (the block). Transactions are recorded into this public database through consensus across a network of decentralised computers, which is achieved by a proof-of-work system called mining.

Many organisations are implementing it already including IBM, Google, American Express, Oracle, Facebook, Ford, Amazon and Nestlé. There are also blockchain-specific companies offering blockchain solutions for supply chain, social media and stock control. These companies often use crypto-utility tokens within their ecosystem. There are also blockchain-based coins with no other use than that they seek to behave in a similar way to traditional currency and to potentially replace it. Whether a utility token or currency coin, both of which fall into the category of cryptocurrency, most are available for purchasing as investment or as a way of speculating on various exchanges globally.

> Dhofar Bank in Oman has already implemented the Ripple blockchain

Hacking incidents and vulnerabilities

There has already been a number of major and high-profile hacking incidents which has government regulators concerned. When it comes to hacking, it is not so much

> When it comes to hacking, it is not so much the cryptocurrencies that are the problem, but rather the exchanges on which they are traded and the digital wallets where many of them are held

the cryptocurrencies that are the problem, but rather the exchanges on which they are traded and the digital wallets where many of them are held.

Many exchanges are unregulated or loosely regulated at best. Their governance standards and cybersecurity measures are severely lacking, which is where the problems lie. Some exchanges have been hacked in recent years. Interestingly, hacking risk is also one of the main concerns for the existing banking system, which means fiat and cryptocurrencies have the same security concern. For instance, online banking apps can be exposed to hacking which aims to steal users' login data and debit or credit card information.

A potential solution to hacking incidents on exchanges is the introduction of decentralised exchanges, essentially a cryptocurrency exchange on the blockchain. This would reduce hacking significantly. Unfortunately, it is not currently practical, due to poor user interfaces, but it could become the standard of the future, especially if regulation supports this innovation.

While it is difficult to govern cryptocurrency itself, and due to the fact that cryptocurrency is apparently unhackable, what policymakers should focus on is the regulation of the services associated with the use of cryptocurrencies. Regulation should focus on stricter business practices within exchanges to avoid fraud and scams, as well as introducing minimum but high standards of cyber risk requirements in order to protect against hacking, phishing and other cyber-related attacks.

Most people involved with the technology agree that blockchain networks are virtually unhackable although some argue that all "software" is vulnerable. The one vulnerability that everyone agrees on is that blockchain technology can be hacked through a mechanism called 51 per cent attacks. This happens when 51 per cent of a network is owned by the same group of people, enabling them to manipulate transactions on what is effectively no longer a decentralised network. While this is possible on some of the very low market cap coins and tokens, it is highly expensive, and some would suggest impossibly expensive, on larger market cap coins such as Bitcoin. According to the CEO of a new blockchain company in Oman, who we interviewed, aside from a 51 per cent attack, no one can hack a blockchain. The CEO echoes the sentiment that vulnerabilities tend to exist in the applications that use blockchain technology such as exchanges and wallet.

Blockchain and financial services

Various studies suggest that implementing blockchain in the banking industry alone could decrease expenses by $20 billion by 2022.

> **Ninety per cent of cyberattacks come from human error and social engineering – a risk that blockchain would be unable to remove**

In addition, the technology could boost the safety of customers' data in a business. Many policymakers in the banking and finance sector already believe that blockchain technology could replace the existing SWIFT transfer system in banks.

According to the IT department of Dhofar Bank in Oman who we spoke to, the bank has already implemented the Ripple blockchain. They said it provides a better experience for international money remittances, increased security against cyberattacks, an improved speed of transfers and is more cost-efficient. The bank added that it did not see any unique challenges in implementing blockchain solutions compared with other technologies.

A significant indication that blockchain is being embraced by banks came from JP Morgan, when they announced their blockchain project, JPM Coin. It has already been approved by 75 banks, such as Santander Bank, in order to enhance the testing process. JP Morgan believes it will help to reduce costs, increase security and improve the speed of financial transactions.

Other sectors

A number of countries, such as Estonia, Slovenia, Malta, UAE and France, are actively promoting blockchain technology by implementing positive regulation and encouraging start-ups to set up in their countries. They clearly see the benefit that the reduction of transactions and middlemen can bring with a database that is apparently tamper-proof and auditable.

There is a particular focus on cybersecurity. As universities, governments, companies and major projects add more security cameras and sensors that require communication of data across device networks, there is an increased need to protect their networks from hackers. This is also true of the internet of things, which sees devices such as fridges, coffee machines and heaters sending data across networks.

Cybersecurity in retail is another area that blockchain could help. Retailers have a long history of using prepaid and loyalty cards, and blockchain provides an excellent opportunity to offer a more secure gift card and loyalty programme that is not exposed to the same data breaches from hacking incidents that has plagued the industry for years. Many suggest that blockchain could also be the solution that Elon Musk needs to get autonomous cars on the road. The threat of terrorists hacking self-driving cars, robots, drones or automated transportation systems in itself is a scenario that would strike fear in any government. Blockchain could provide a solution not only to the hacking threat but also to potential accidents arising from other challenges too, such as the current lack of accuracy of verifying of data collected from the surrounding environment and potential downtimes and systems failures that are inherent in a centralised network.

Challenges

One of the major drawbacks of the technology is the need for mining, which essentially requires computing power. It has been estimated that during a week, the entire blockchain network consumes energy on a par with the total amount of electricity used by Hungary – or 0.25 per cent of the entire planet's energy needs. Recent research estimated that mining could account for 1 per cent of global energy usage by 2020, an amount that would increase rapidly through mass adoption.

Blockchain technology is improving and a number of updates have already made many blockchains more energy efficient. Nonetheless, it should be a concern for governments looking to reduce carbon emissions. Regulation could be introduced to ensure that mining companies adhere to strict renewable energy requirements, although this will also potentially shift mining activities to countries who have less stringent rules on mining activity (and cheaper electricity).

A fully decentralised system would enable users to trade, transfer and receive money directly without intermediaries. It could be argued that some intermediaries may be seriously exposed financially or resist the technology. As a result of this, and in countries or cities largely reliant on the financial sector, unemployment rates could rise, and policymakers therefore need to think about whether creating new roles for intermediaries may be possible in order to avoid this scenario.

There is also the matter of investor and customer protection to consider. The existing centralised financial system has a level of trust built into it that protects money in events such as bankruptcy, fraud or in the event of the death of a family member. This level of protection does not exist in a decentralised system. It seems as though the most likely scenario is a semi-decentralised system, which could therefore still be potentially more vulnerable to cyberattack.

What about GDPR?

A major area of concern for all businesses over the past couple of years has been the General Data Protection Regulation (GDPR), introduced in May 2018 to increase people's data privacy. It presents a possible stumbling block for blockchain implementation. The major areas of conflict include the fact that blockchain would hold personal data that is publicly accessible at the same time as not allowing for changes, such as deletion as per requirements of GDPR under "the right to be forgotten".

This is a direct clash of function. However, by ensuring that the blockchain does not hold any personal details, such as individual names, there may be a way to get around this problem. Additionally, GDPR does not aim at regulating technologies as such, but regulates how organisations use these technologies.

Both GDPR and blockchain's main focus is the protection of data, something which blockchain does very well as we have already discussed, and as a result, while initially it may seem that they are incompatible, blockchain could actually be a potential solution to meeting the GDPR requirements of encryption. Additionally, one of the reasons for the existence of GDPR was the misuse of data by major corporations, something that the decentralised nature of blockchain totally removes from the equation.

The same, but different

A blockchain future with levels of security we have previously not been used to seems difficult to imagine. We have grown accustomed to major cyberattacks and breaches. While blockchain, if embraced and implemented properly, is certain to reduce these attacks significantly, we will still be faced with a fact not yet mentioned in this article. Ninety per cent of cyberattacks come from human error and social engineering – a risk that blockchain would be unable to remove. As technology moves forward, humans seem to be unable to adapt quickly enough. The staggering speed of innovation could mean that while the future may turn out to be very different to today, many of the same old threats could remain.

This article was written by Alexander Larsen CFIRM, president of Baldwin Global Risk Services Ltd, and Faisal Alnahdy, senior auditor at the State Audit Institution in Oman. It is based on Alnahdy's MSc dissertation, "Evaluation of risks associated with cryptocurrency: case study on Oman", which he wrote at Glasgow Caledonian University.

> **It has been estimated that during a week, the entire blockchain network consumes energy on a par with the total amount of electricity used by Hungary**

Cookie cutters

Last year's reform of Europe's data protection regulations is soon to be extended to electronic communications, including those governing website cookies and marketing emails

BY JAMES CASTRO-EDWARDS

Data protection law is in a state of change. After years of negotiation, the General Data Protection Regulation (GDPR) finally took effect on May 25, 2018, to unprecedented publicity for a piece of legislation. Few UK citizens between the ages of 16 and 60 with access to a computer or smartphone will have escaped the bombardment of emails, asking them to "re-consent" to staying in touch, purportedly to comply with the GDPR.

However, the GDPR is not the only area of data protection reform. The legislation that governs certain aspects of electronic communications (including the unsolicited marketing emails that were the subject of the requests to "re-consent") has also been the subject of review. The European Commission (EC) had originally intended for the ePrivacy Regulation (the ePR) to take effect at the same time as the GDPR. The ePR currently remains a work in progress, but, when it does become law, businesses will need to be prepared for the changes that it will introduce.

> The most broadly applicable changes concern the use of cookies, and unsolicited direct marketing

Electronic communications

The ePR is a draft piece of legislation proposed by the EC which is intended to update the law governing certain aspects of electronic communications networks and services. The new regulation would replace

> **The ePR is a draft piece of legislation proposed by the EC which is intended to update the law governing certain aspects of electronic communications networks and services**

the ePrivacy and Electronic Communications Directive (2002/58/EC), which is implemented in the UK by the Privacy and Electronic Communications Regulations (EC Directive) 2003 (as amended) (PECR).

To understand the changes the ePR would introduce, it is helpful to have a basic understanding of Directive 2002/58/EC and PECR. While the GDPR regulates the processing of personal data generally, Directive 2002/58/EC and hence, in the UK, PECR sits alongside the GDPR and regulates a number of specific areas related to electronic communications. Directive 2002/58/EC (like any European Directive) requires each European Member State to implement its provisions through national law, so that each Member State has in place equivalent legislation to PECR; though in practice, there are differences from country to country.

The areas regulated by PECR are electronic marketing (marketing by electronic means, including telephone, text, email and fax); cookies (the use of cookies to track individuals' use of websites and electronic services); security (the security of public electronic communications services); and privacy (the privacy of customers using communications networks and services).

In the UK, organisations must handle personal data (i.e. information about living individuals) in accordance with the GDPR. Organisations that use cookies, carry out direct marketing by electronic means or operate electronic communications services must also comply with PECR. This position will be largely the same in other EU Member States. Most UK businesses have a company website, many of which use cookies, and most businesses carry out some degree of marketing, which must comply with PECR. PECR has been amended seven times, most recently in 2018 to ban cold-calling of claims management services and to introduce directors' liability for serious breaches of the marketing rules, and in 2019 to ban cold-calling of pensions schemes in certain circumstances.

The EC is in the process of replacing Directive 2002/58/EC with the ePR, which was originally intended to take effect at the same time as the GDPR on May 25, 2018. However, the ePR has not yet been finalised.

Preparing for change

The EC published a draft proposal in January 2017, which included seven main changes to the law governing electronic communications networks and services (see *Main proposed changes under ePR*). After extensive lobbying, the European Council issued a revised draft in July 2018, which included significant changes, in particular around the information that must be provided to users about third-party cookies, and the requirement to make individuals select privacy settings each time that new options become

MAIN PROPOSED CHANGES UNDER THE ePR

1. **Scope:** The ePR will apply to all providers of electronic communication services, including "over the top" services such as WhatsApp, Skype and Facebook Messenger, which will be governed by the same legislation as traditional telecoms operators. The regulation will apply to non-EU service providers that provide electronic communications services to individuals in the EU.

2. **Confidentiality:** Electronic communications must be confidential and secure, and any interference such as listening, tapping, intercepting, scanning or storing communications is prohibited without users' consent. Consent must be established to the standard required by the GDPR. However, processing for exceptional purposes such as safeguarding the public interest, national security or criminal law enforcement will continue to be permitted without users' consent.

3. **Content and metadata:** The ePR will apply to both communications content and metadata. Data such as numbers called, call duration, websites visited and geographical location will need to be deleted or anonymised if users have not given their consent, except for certain specified purposes such as billing. However, the regulation will permit telecoms providers to use this information for a broader range of services (subject to having obtained users' consent), thereby providing businesses with the opportunity to develop and offer new services.

4. **Unsolicited electronic direct marketing:** The ePR will require users' consent for any type of unsolicited marketing communication, including by telephone, email and text message, though the "soft opt-in" will continue to enable businesses to market similar products and services to existing customers. The position regarding B2B marketing appears likely to remain the same as it is under Directive 2002/58/EC, which has been interpreted differently by EU Member States, but in the UK means that opt-in consent is not required from "corporate subscribers".

5. **Marketing caller ID:** The new regulation will allow Member States to stipulate that marketing callers cannot block their caller ID, or should use a special prefix which indicates that they are engaged in marketing.

6. **Cookies:** Users' consent will no longer be required for non-intrusive cookies which improve the user's internet experience (for instance, remembering shopping cart history). Any non-essential or third-party cookies are likely to require the end-user's consent. Further, the ePR is intended to enable users to give consent by changing certain settings on their internet browser so that they will not need to consent to cookies every time they visit a webpage.

7. **Penalties:** The ePR will enhance enforcement, bringing the penalties into line with those of the GDPR.

Source: *James Castro-Edwards*

> "Businesses that carry out electronic marketing and use cookies on their website can get a head start by reviewing their marketing activities and auditing their website cookies

available. A further revised proposal was published on March 13, 2019, though negotiations remain ongoing.

While the draft regulation remains the subject of negotiation, it is impossible to state with certainty the steps that businesses must take in order to comply with its requirements. Some of the changes the ePR would introduce are specific to communications services providers and hence will not be relevant to all businesses. However, the most broadly applicable changes concern the use of cookies, and unsolicited direct marketing.

Most businesses are likely to be engaged in marketing activities to some extent, and most businesses will operate a website that is likely to use cookies. These organisations can take the first step towards preparing themselves for the ePR by reviewing their marketing activities and use of website cookies.

In reviewing their marketing activities, companies should consider their marketing channels – such as telephone, email, text message and social media – their contact base (i.e. whether contacts are B2B, B2C, existing customers) and where their personal data were obtained from. Note that companies must be particularly careful with bought lists of contacts, which are problematic under the GDPR. Where businesses rely upon contacts' consent, they must ensure that any purported consent meets the requirements of the GDPR – it is freely given, informed, specific and indicated by an unambiguous indication and so on.

In relation to cookies, businesses need to identify the cookies that they use, which may require a website audit (if the business operates a number of websites), and a cookies audit to identify and categorise all the cookies used on its websites.

Key risks

The ePR will apply to any business that provides any communication services to individuals in the EU. This applies to both businesses established in the EU and those outside the EU that are providing the services within the EU. It also applies to any business using cookies or similar tracking technologies on devices within the EU.

As the regulation will effectively apply to any internet-facing business providing services within Europe, it is likely to have a similar impact to the GDPR and will be felt globally. The impact of this is that all affected businesses will need to review their online standards of privacy to ensure that these comply with the new rules (once they are finalised).

One of the proposed changes the ePR would introduce is that non-compliance will be subject to sanctions of the same magnitude as those of the GDPR. The proposed penalties for breaches of the ePR would range from up to €10,000,000 or 2 per cent of worldwide annual turnover for breaching the provisions relating to the protection of end-users' information and unsolicited and direct marketing communications, and up to €20,000,000 or 4 per cent of worldwide annual turnover for infringing the principle of confidentiality of communications and time limits for erasure.

Based on past experience, there is a real likelihood of enforcement action for breaches of the ePR. In the UK, around half of the enforcement activity of the Information Commissioner's Office (ICO) arises from breaches of PECR. Non-compliant electronic marketing typically affects large numbers of individuals, and due to a more informed public and simple reporting mechanisms on the ICO website the result is a greater volume of complaints. ICO investigations are frequently prompted by complaints, and the greater the number of complaints, the greater the likelihood of intervention, so non-compliant marketers face a genuine risk of enforcement action.

How risk managers can help their organisations

It would be impossible to give definitive advice on compliance until the ePR has been finalised; however, risk managers can help their organisations by taking three key steps around awareness, application and preparation.

First, risk managers should ensure that the business is aware of the ePR, is kept informed of developments and is kept abreast of when it is likely to come into force. While the precise rules may still be subject to further amendment, as mentioned above, there are steps that businesses can start taking now to put themselves in the best position. Second, while specific details are yet to be finalised, businesses should be able to identify in broad terms the parts of the regulation that are likely to apply to them. Organisations should already have a general idea of the extent to which the new rules around direct marketing, website cookies and electronic communications services will apply to them. Finally, businesses that carry out electronic marketing and use cookies on their website can get a head start by reviewing their marketing activities and auditing their website cookies.

Risk managers that have taken the above steps should continue to watch this space, so that when the ePR is eventually finalised, they are ready to respond quickly and implement appropriate compliance measures.

James Castro-Edwards is a partner at Wedlake Bell LLP and leads the firm's outsourced data protection officer service, ProDPO (prodpo.com).

> **"The ePR will enhance enforcement, bringing the penalties into line with those of the GDPR**

Changing the climate on risk

Risk managers can take a proactive approach in helping businesses get a practical grip on climate change risk

BY GARETH BYATT AND SARAH GORDON

Around the world, the call to action to address climate change is louder than ever. In the UK, for example, the government issued its Carbon plan in November 2018, setting out a vision for a low-carbon economy. Businesses in all industries, in the UK and elsewhere, are looking at how they can chart and navigate a course to deliver successful climate change action and carry out their activities in a sustainable way.

The signals are clear to see. Driven by many factors including public demand and demonstrations, intergovernmental agreements, changing national government policies, and investor and shareholder demands, the global economy is shifting and repositioning to respond to climate change as part of the broader picture of sustainability.

We believe risk managers should be working with their boards, executives and management teams to develop strong, risk-informed climate change strategies and actions that lead to good business performance.

> **Risk managers should be working with their boards, executives and management teams to develop strong, risk-informed climate change strategies**

Investors and shareholders

Investors and shareholders have an important role to play in our strategy and operational considerations. We

Image credit: Nicole S Glass / Shutterstock.com

> **For some risk managers and risk teams, the climate change agenda may still feel somewhat removed from what they do in their day-to-day work**

have spoken recently with a leading Environment, Social and Governance (ESG) research firm Sustainalytics to gain some perspectives about this.

Investors and shareholders around the world are increasingly vocal and actively engaging with the businesses they invest in. Many are increasingly choosing to place the funds they control into businesses, across all industries and sectors, that are visibly demonstrating positive climate change action. In addition, strong climate change strategies result in good business performance.

The impact is happening right now – funds are moving away from businesses that do not show an appropriate degree of commitment to climate change. Boards and executive teams around the world today recognise that they need to show their businesses are a compelling long-term investment for the organisations that provide funding to them.

Driven by an increasing adoption of recommendations from influential institutes including the Task Force on Climate-related Financial Disclosures (TCFD) and the UN Principles for Responsible Investment (PRI), investors are moving away from looking at the carbon footprint of businesses and towards a more holistic understanding of the carbon exposure that businesses have, and their risk management and transition strategies to address it.

Investor demands to understand the carbon exposure of businesses they invest in are broad. Investors are looking at a wide range of exposure to material climate change risks, according to Sustainanalytics. These include aspects of carbon impact in companies' operations, as well as risks derived from the products and services they produce; involvement in fossil fuels, and exposure to stranded assets; the carbon impact of operational risks; non-carbon emissions, effluents and waste; human capital; occupational health and safety; relations with local communities; and business ethics and corporate governance (including anti-corruption, lobbying, fair competition, board independence and shareholder rights).

Coupled with this, the number of ESG and climate change driven shareholder proposals and resolutions on climate change is growing fast. Shareholder action is forcing the very largest businesses to make commitments on climate change targets. Some businesses are ahead of the game and using good risk management to drive this change themselves.

> **Social and sustainability bonds may be worthwhile financing options to explore**

A role for sustainability and risk teams

For some risk managers and risk teams, the climate change agenda may still feel somewhat removed from what they do in their day-to-day work. However, we would like to suggest that this should not be the case today for risk managers in any organisation. Risk managers should be helping their sustainability and ESG teams (SESG in this article), as well as their executive and management teams, to work out the best climate change strategy and to agree how to measure, manage and report material climate change risks openly to investors and shareholders. Good risk management in climate change, as part of a broader focus on sustainability, can lead to good business performance.

Some businesses today are housing their risk and SESG functions under the same executive. Whether this is the case or not, there are many compelling reasons to ensure the risk function is working closely with the SESG function.

To work effectively with the SESG experts on climate change, risk managers have to go deeper than attending occasional "think tank" reviews and cross-functional meetings, and providing "a helping hand" with some workshops every now and then. They have to develop a plan with the organisation's SESG experts to assist executives in identifying, assessing, quantifying and prioritising the climate change risks the organisation faces to achieving its objectives – and to help shape a strategy and practical actions to make it happen. We believe risk managers and risk teams are well positioned to do this because they have a broad reach across their organisations. This reach means risk professionals can play a valuable role in liaising with executives, functions, offices and operations teams.

There are four key areas we believe risk managers and risk teams can help their organisations realise value in by addressing climate change: developing risk-informed climate change and ESG strategies, considering sustainable financing options, helping people implement climate change and ESG strategies, and collaborating with other businesses to share knowledge.

Risk-informed strategies

Risk managers can work with their organisation's SESG teams and executives to build a strategy and a framework / management system. By working closely with the SESG team on the risks the organisation faces and to develop a risk-informed strategy, risk managers will help their executives and board to agree on actions to harness opportunities and manage threats.

There are many ways to help in this process. Risk managers can review the organisation's top business risks through the lens of climate change and ESG to fully understand each risk component. To support this process, risk managers may choose to engage with external ESG experts to understand how they view the organisation's ESG and climate risks.

Risk managers can interview key stakeholders across the organisation and include in those meetings (or separately interview) investors, analysts, insurers, business partners, clients, governments and industry associations, and of course the risk function's own teams and staff. For instance, many insurers have sophisticated climate change models which risk teams may be able to leverage to assist with risk-informed decision-making in the business strategy.

This approach can be coupled with scenario analysis to consider what different climate change risks could eventuate in and what their impact to the business could be – in terms of both opportunities as well as threats.

In addition, risk managers can agree what the organisation's climate change risk appetite needs to be and how that should be embedded across the organisation, and work with the legal team to understand where legislation in the jurisdictions where the business is operating is heading, as well as using risk tools and techniques to anticipate the needs of investors and shareholders and work out with executives how to show them a compelling risk strategy. That would include understanding the ESG reporting methods of leading ESG analysts and deciding how to use them to challenge, innovate and continuously improve the business, and learning from organisations that are leading the way.

If the organisation is not already doing so, risk managers should investigate adopting the TCFD as a method of financial disclosure (if the organisation is large enough), and research how to leverage other global institutes such as the UN's PRI, the Climate Action 100+ initiative and other industry-specific bodies that provide advice and accreditation mechanisms.

Taken together, these approaches can be used to create powerful business plans and external-facing reports on what the organisation is doing in this area.

Sustainable financing options

Risk managers can also work with their SESG teams and finance and treasury teams to help executives understand and assess the viability of sustainability-performance-linked investment loans. Such loans, in which performance is measured against a set of ESG criteria, may help the organisation demonstrate its "strategy in action", through a commitment to achieve climate change targets, and to receive financial backing for pursuing such a strategy. Social and sustainability bonds may be worthwhile financing options to explore.

Organisations may benefit by using independent performance ratings in investor roadshows – for example, for debt and equity financing, and for reporting to shareholders and stakeholders, suppliers and customers.

Implementation

Embedding a risk-informed climate change and ESG strategy across the organisation, as part of a broader sustainability strategy, is of course the proof of the pudding. Risk managers can play a key role in this initiative.

Risk managers can use the agreed strategic risk appetite to define with the operations teams, in detail, the risks the business is willing to accept and take to pursue its objectives. This will entail agreeing how the business teams will implement actions to manage risk appetite successfully. Risk managers can also help operations teams to capture and quantify specific climate change risks and actions in their business plans, as well as using operational scenario analysis to consider the range of scenarios that are possible for operations to achieve targets and match them to the risk appetite. When operations have key decisions to make that have a climate change implication, it can be helpful to use decision trees to understand different operational options that are available, and to select which ones are best.

Getting people talking about and challenging themselves on the risk appetite for climate change impacts can help raise awareness – as can holding workshops to agree risk-informed actions, including with suppliers (who are key partners in achieving the strategy).

Finally, risk managers can work to ensure risk-informed decision-making is embedded into day-to-day operational activities and to find the balance between opportunities and trade-offs in, for example, how the organisation manages water, energy and waste.

Collaborate

Risk managers should become advocates for risk-informed climate change, and the broader matter of sustainability, with peers in other businesses, across different sectors, and in industry forums. Seeking out examples where businesses are working successfully to address climate change and exploring how to emulate that success can be effective. The risk team should share its own successes to help spread best practice.

It takes a concerted effort to be fully engaged in helping an organisation to address climate change and ESG, but it has positive benefits for the risk team. The right risk tools and techniques can help organisations set and implement a good climate change strategy. Second, demonstrating sound risk management to investors in this area can help the business secure funding. In addition, using smart financing options positions the organisation to use intelligent sources of finance. Finally, it demonstrates the value of the risk team being at the heart of organisational strategy and operational management.

Taking the approach outlined here may mean risk managers have to reassign or change their focus on other priorities. Nonetheless, we believe addressing climate change is one of the most important contributions that risk managers can make to our organisations today.

Gareth Byatt APAC is IRM Global Ambassador and a director of Satarla, Australia, and principal consultant at Risk Insight Consulting. Dr Sarah Gordon IRM Cert is an IRM Trainer and managing director at the global risk consultancy and training provider Satarla. They are involved with the IRM on various fronts.

> **The risk team should share its own successes to help spread best practice**

Conflicts over discrimination

Protecting an organisation's good reputation should never be an excuse for discrimination in the workplace, says Nick Chown

Diversity risk often ranks low on organisations' risk registers. This fact was highlighted in the IRM-backed report *Perspectives of global corporations*, by the Cambridge Centre for Risk Studies. "Gender and diversity risk is ranked at the bottom of risks by survey respondents across all sectors," it said. "Despite its low prioritisation, we believe its growing visibility makes it worth highlighting in this report." While the report itself focused on equality issues, it noted that "there is growing consensus that greater diversity in the workplace correlates to improved business performance." The IRM agrees that the benefits of diverse thinking in enhancing organisational decision-making are well established.

My Metropolitan Police team was voted European risk management team of the year in 2008 due largely to the fantastic work of an autistic colleague, whom, incidentally, I was warned against including in the team. Since then, I have become an autism specialist. My work in autism involves research, advocacy, mentoring and training provision.

Reputation vs discrimination

It is important to understand that the management of risks to reputation and discrimination can be in conflict. The conflict arises because of a risk of managing reputation *risk* at the expense of *actual discrimination*. It can be argued that reputation risk is the highest priority of all for many organisations. So, for those organisations, management of key risk areas such as discrimination may be prejudiced where there is a conflict with reputation risk.

I am well aware of the importance to organisations of their reputation, which requires high priority being given to the management of reputation risk. Yet all of my autism work is focused firmly on improving the lived experience of autistic people, including while they are at work. The importance of the risk of discrimination and its management in this context cannot be over-emphasised.

For example, a colleague, a consultant clinical psychologist, was told by their employer not to disclose to their clients that they are autistic. The reason given was that disclosure could lead to damage to the organisation's reputation. In my time as a corporate risk manager, before finding out that I am autistic and learning about autism, my advice to the employer in my colleague's situation might well have been to do precisely the same.

Regard for the law

Setting aside the discriminatory attitude this is indicative of, there is a risk issue here. The issue of what autism is remains a matter of much debate, but it is defined as a disability under the Equality Act. This act makes discrimination against disabled employees illegal. Discrimination involves someone being treated differently

> **"The management of risks to reputation and discrimination can be in conflict**

and not as well as other people because of their disability. To the best of my knowledge, there is no legal requirement for an organisation to manage its reputation risk, although they would be negligent not to do so of course.

It might also be argued that the potential for adverse publicity represents a serious risk to a business whereas discriminating against an employee and clients is unlikely to have any significant adverse effect on the organisation. But the latter is legally and morally wrong and should be at odds with an organisation's values – just as the action taken by my colleague's former employer was a clear breach of theirs. That is why discriminating against staff in the name of a good reputation threatens to undermine the very goal such behaviour is intended to achieve.

Dr Nick Chown FIRM is a leading author and researcher into autism and former director of risk management at the Metropolitan Police. Contact: npchown@gmail.com

Due diligence solutions

Minimise risk by maximising the data that supports your most critical business decisions. LexisNexis is a leading provider of aggregated global content and powerful business intelligence tools. Protect your organisation from the risk of heavy fines and damage to corporate reputation by accessing the information you need on people, companies and countries. Our cost effective and flexible product modules include: PEP, sanctions, watch list and negative news screening. Enhanced due diligence and reporting. Proactive supply-chain and third-party risk media monitoring. Outsourced due diligence, compliance and risk advisory. Content integration and data feeds (APIs) into proprietary systems.

Rebecca Gillingham
+44 (0) 20 7400 2809
bis@lexisnexis.co.uk
bis.lexisnexis.co.uk
LexisNexis
30 Farringdon Street
London
EC4A 4HH

Empowering your resilience

C2 is an established Business Continuity software provider with a continuing commitment to its customers to evolve with the market. Our mission is to provide intuitive and innovative solutions for the global business resilience market and reshape the industry as we know it today. Our Business Continuity Software is used to alleviate and assist with the day to day management of an organisation's Business Continuity Management System requirements. We provide BCM software and practical solutions to some of the world's largest utility companies, world leading finance and investment organisations, global telecom organisations and more. Find out more: https://continuity2.com/

Richard McGlave
+44 (0) 845 094 44 02
info@continuity2.com
continuity2.com
Prism House, Scottish Enterprise
Technology Park
East Kilbride, Glasgow, UK
G75 0QF

Enterprise risk management and risk analysis software

riskHive are an established global provider of professional cloud, intranet and desktop solutions for the management and analysis of RAID (risks, issues, assumptions and dependencies). Being low maintenance, highly configurable and cloud based, the Enterprise Risk Manager application can get you online in under 24 hours, supporting your existing processes and terminology. Easily import existing risk information to quickly produce a consolidated risk portfolio. Relied on by customers ranging from New Zealand through the Middle East to Northern Europe riskHive deliver a truly global ERM solution with a truly enterprise 'all-in' licence.

Ian Baker
+44 (0) 1275 545874
ian.baker@riskhive.com
www.riskhive.com
riskHive Software Services Ltd.
Dilkush, Farlers End
Bristol
BS48 4PG

Financial risk management and Solvency II software

RemitRix helps insurers manage financial and actuarial risks by harnessing the power of Machine Learning to improve actuarial predictions. Our product RemitRix Agile is a web based financial risk management platform. RemitRix Agile includes classical risk management tools such as ESG, VaR, Solvency II full solution, optimization tools and more. It is easy to deploy and manage. It is planned to fully integrate with our future actuarial solution.

Effi Mor
+44 (0) 20 3608 3987
info@remitrix.com
www.remitrix.com
RemitRix
Shoham Street 8
Ramat Gan
Israel

Risk and audit management software solutions

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

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

Risk, insurance and safety technology solutions

Ventiv Technology is the preeminent provider of global risk, insurance, and safety technology solutions. Working in partnership with our clients to understand their challenges and key business objectives, our solutions adapt to your precise needs and evolve with you. Providing a central platform to work across your company and functions to eliminate silos and help embed risk management. Delivered with Ventiv's extensive risk management and technology experience to provide unsurpassed client value and operational excellence. Ventiv pride themselves on data security and have recently added another certification to their tool belt – ISO27018:2014; standard for protecting privacy in the cloud.

Steve Cloutman
+44 20 3817 7373
steve.cloutman@ventivtech.com
www.ventivtech.com
Ventiv Technology
30 Eastcheap
London
EC3M 1HD

Risk management software

AgenaRisk is a model design and execution environment for Bayesian Networks, designed for organisations that need to assess and manage risks in areas where there is little or no data, where direct measurement is not possible, and in the face of new, often novel, circumstances. Organisations use AgenaRisk to model a variety of problems including operational risk, actuarial analysis, intelligence analysis risk, systems safety and reliability, health risk, cyber-security risk and strategic financial planning. Models developed in AgenaRisk can be integrated into a wider service using AgenaRisk Developer and ultimately deployed using AgenaRisk Enterprise.

Ed Tranham
+44 (0) 1223 263880
sales@agenarisk.com
www.agenarisk.com
11 Main Street
Caldecote
Cambridge
CB23 7NU

Risk management software

ALYNE – is an industry leading and award-winning, Regulation Technology Software company – that makes it easy for organisations to reduce the cost – of managing risk and compliance obligations and is built by industry experts. ALYNE – is a next generation, cloud solution that makes risk and compliance management as easy as browsing social media. ALYNE – with its unique pre-built library of controls, integrated risks and assessment templates – mapped to regulations and standards, is ready to use out of the box – with dynamic reporting and real-time risk insights. ALYNE's – innovative approach – enables organisations to make the right executive decisions and outcomes – and to drive business advantage.

Pierre Silavant
+44 (0) 7767 444 755
pierre.silavant@alyne.com
www.alyne.com
41 Luke Street
Shoreditch
London
EC2A 4DP, UK

Risk management software

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

Trevor Williams or Verna Hughes
+44 (0) 203 713 4590
info@magiquegalileo.com
www.magiquegalileo.com
Magique Galileo Software
Birchin Court
20 Birchin Lane
London, EC3V 9DU

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

The Protecht Group is a leader in Enterprise Risk Management Software and Services that enables organisations to achieve their strategic objectives through efficient, effective and agile Risk Management. Protecht. ERM™, Protecht's flagship product, has been deployed in a SaaS model since development commenced in 2002 and remains ahead of the curve on innovation and functionality. Used by government agencies, regulators, commercial and not-for-profit organisations of all sizes and risk maturity, Protecht. ERM™ allows companies to seamlessly integrate risk management into their day-to-day activities and gain operating efficiencies through its flexible web-based forms, workflow engine and highly adaptable reports and dashboards. Protecht is more than a software company, we guide you through your risk management journey.

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

Risk management software

Xactium is a cloud based GRC software provider that helps Risk Managers to transform the way that organisations value and manage their enterprise risk. As the central risk platform used by the FCA to supervise the market, it has also been adopted by a wide range of financial organisations such as Direct Line Group, JLT, MS Amlin, Leeds Building Society and Argo Group. Xactium is the world's first enterprise risk-intelligent system, with the revolutionary use of embedded AI (Artificial Intelligence), 3D visualisation and automation that dramatically improves efficiency and creates innovative analytics. Reporting is made easy and timely, and predictive insights enable senior managers to prioritise resources. Overall, Xactium releases more time and resource for the risk team to help promote best practice and demonstrate the value of risk across the business through actionable insight.

Steve Birch
+44 (0) 114 2505 315
steve.birch@xactium.com
www.xactium.com
Xactium House
28 Kenwood Park Road
Sheffield
S7 1NF

Young ones

A new study shows that younger people are unimpressed with everything from politics to business. What will happen when they begin to enter senior management roles?

Disillusion is the key tone of a new report on attitudes of people often shoe-horned into the sociological groups known as the millennial generation and Generation Z, according *The Deloitte global millennial survey 2019*.

In fact, the results of the survey are bad news from the outset. "They're not particularly satisfied with their lives, their financial situations, their jobs, government and business leaders, social media, or the way their data is used," the report announced.

The age range is one clue to this malaise. The groups' members were born between the years 1983 to 2002 – the oldest coming into the workforce at around 2000 at the earliest. That means that most have been caught up in the financial crisis and its austerity aftermath all of their working lives.

"In the United States," the report says, "millennials who entered the labor market around the recession, or during the years of slow growth that followed, experienced less economic growth in their first decade of work than any other generation." Social media, political change, technological disruption and other factors have increased a growing sense of disconnection.

> There were strong correlations between those who plan to stay in their current jobs and those who said their companies deliver best on financial performance, community impact, talent development, and diversity and inclusion

Top priorities

Top of the personal concerns for both groups are climate change, unemployment and income inequality (although terrorism scored second for Generation Z respondents). While most (36 per cent) say government has most responsibility to improve social mobility, businesses came second place (20 per cent).

Although businesses may rejoice that they get off lightly in this respect, millennials most commonly believe businesses should prioritise the production of high-quality goods and services (36 per cent) and generate jobs (35 per cent). Over half (55 per cent) see generating profit as business's main achievement, whereas fewer than one in three think this should be the case – yet another cause of disillusionment.

Under the shareholder value model that still holds sway in the UK and is enshrined in law, a director's primary duty is to make profits for their company's investors – everything else is secondary. While the Companies Act 2006 did add some other considerations, such as treating suppliers fairly, most of the ethical behaviour for businesses listed on the UK stock exchange is contained in principles-based corporate governance guidance.

The option of being ethical could turn into a compulsion as these people mature further. Such less-tangible factors are more important to these younger people – both in terms of what a business stands for and how it treats its workers, suppliers and customers. "There were strong correlations between those who plan to stay in their current jobs and those who said their companies deliver best on financial performance, community impact, talent development, and diversity and inclusion," the report says. Profit is important but it needs to be seen in a broader context if it is to satisfy younger people.

Gig economy

For those businesses that do not meet this challenge, the news is also glum. Four in five survey respondents said they like the idea of a gig economy, suggesting that those talented or motivated enough to do so will go it alone and, in doing so, contribute to the growing skills gaps in large organisations.

Over the next decade, millennials will increasingly start taking executive management roles. As the old guard are replaced, the attitudes expressed in this report about the expected purpose of business and its corresponding ethical behaviour will become mainstream among management and investors alike. Despite long-standing resistance to overturning the shareholder value model in the UK's boardrooms, it could eventually be a reality that is consigned to the history books.