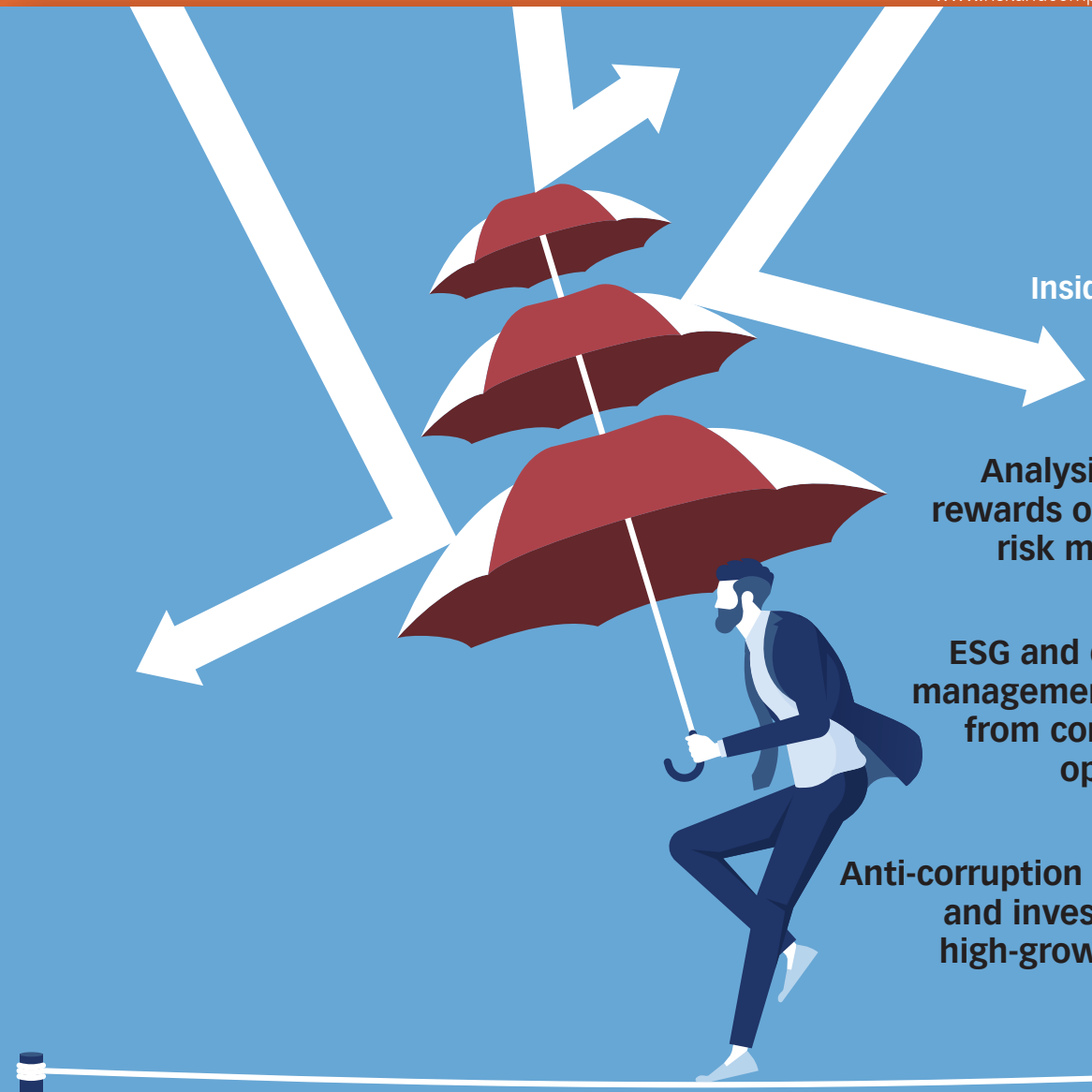
R&C risk & compliance
JAN-MAR 2023
www.riskandcompliancemagazine.com



Inside this issue:

R&C

Editor: Mark Williams
Associate Editor: Fraser Tennant
Associate Editor: Richard Summerfield
Publisher: Peter Livingstone
Publisher: James Spavin
Production: Mark Truman
Design: Karen Watkins

Risk & Compliance
Published by Financier Worldwide Ltd
First Floor, Building 3
Wall Island, Birmingham Road
Lichfield, WS14 0QP
United Kingdom

+44 (0)121 600 5910
riskandcompliance@financierworldwide.com
www.riskandcompliancemagazine.com

ISSN: 2056-8975

Meet your 2023 professional goals
with SCCE's compliance and ethics events

Society of Corporate Compliance and Ethics® (SCCE)® is dedicated to supporting compliance and ethics professionals across the globe with educational events that cover topics relevant to a wide range of roles and industries. We are always adding new events; visit corporatecompliance.org/events for the most current list.

Global In-person Events

11th Annual European Compliance & Ethics Institute
March 20–22 • Amsterdam, Netherlands

Compliance Risk Assessment and Management
April 20–21 • Anaheim, CA

Higher Education Compliance Conference
June 11–13 • Phoenix, AZ

Creating Effective Compliance Training
July 31–August 1 • Orlando, FL

22nd Annual Compliance & Ethics Institute
October 2–5 • Chicago, IL

Basic Compliance & Ethics Academies

Get in-depth, in-person classroom-style learning, ideal for professionals with some compliance experience who are ready to support, enhance, and manage a comprehensive compliance program.

January 23–26 • Orlando, FL
February 27–March 2 • Scottsdale, AZ
April 3–6 • Nashville, TN
May 8–11 • Chicago, IL

Regional Compliance & Ethics Conferences

These one-day educational events explore a diverse spectrum of topical compliance issues.

February 10 • California & Arizona VIRTUAL
February 23 • Alaska VIRTUAL
March 3 • New York & Boston VIRTUAL
April 28 • Tampa, FL IN-PERSON
May 19 • Minneapolis, MN IN-PERSON
June 16 • Chicago, IL IN-PERSON

Virtual Events

Sports, Compliance, and Ethics Conference
January 19

Aerospace, Defense & Government Contracting Compliance & Ethics Conference
February 21

Corporate Compliance Enforcement Conference
March 30

Nonprofit Sector Compliance Conference
May 23

Creating Effective Compliance Training
February 15–16
June 21–22
November 1–2

Compliance Risk Assessment and Management
February 22–23 (Central European Time)
June 26–27
September 27–28
December 12–13

DATES COMING SOON FOR:
Compliance Auditing & Monitoring
Conducting Compliance Investigations
ESG & Compliance Conference

Compliance & Ethics Essentials Workshops

These four-day virtual events feature core compliance and ethics content designed for those new to compliance management or those who have practiced for a few years.

February 6–9
May 15–18
September 18–21
October 16–19 (Central European Time)
December 4–7

Webinars

View our weekly offering of webinars focused on regulatory compliance, enforcement, plan development, and more!

Learn more and register
corporatecompliance.org/events

SCCE Society of Corporate Compliance and Ethics

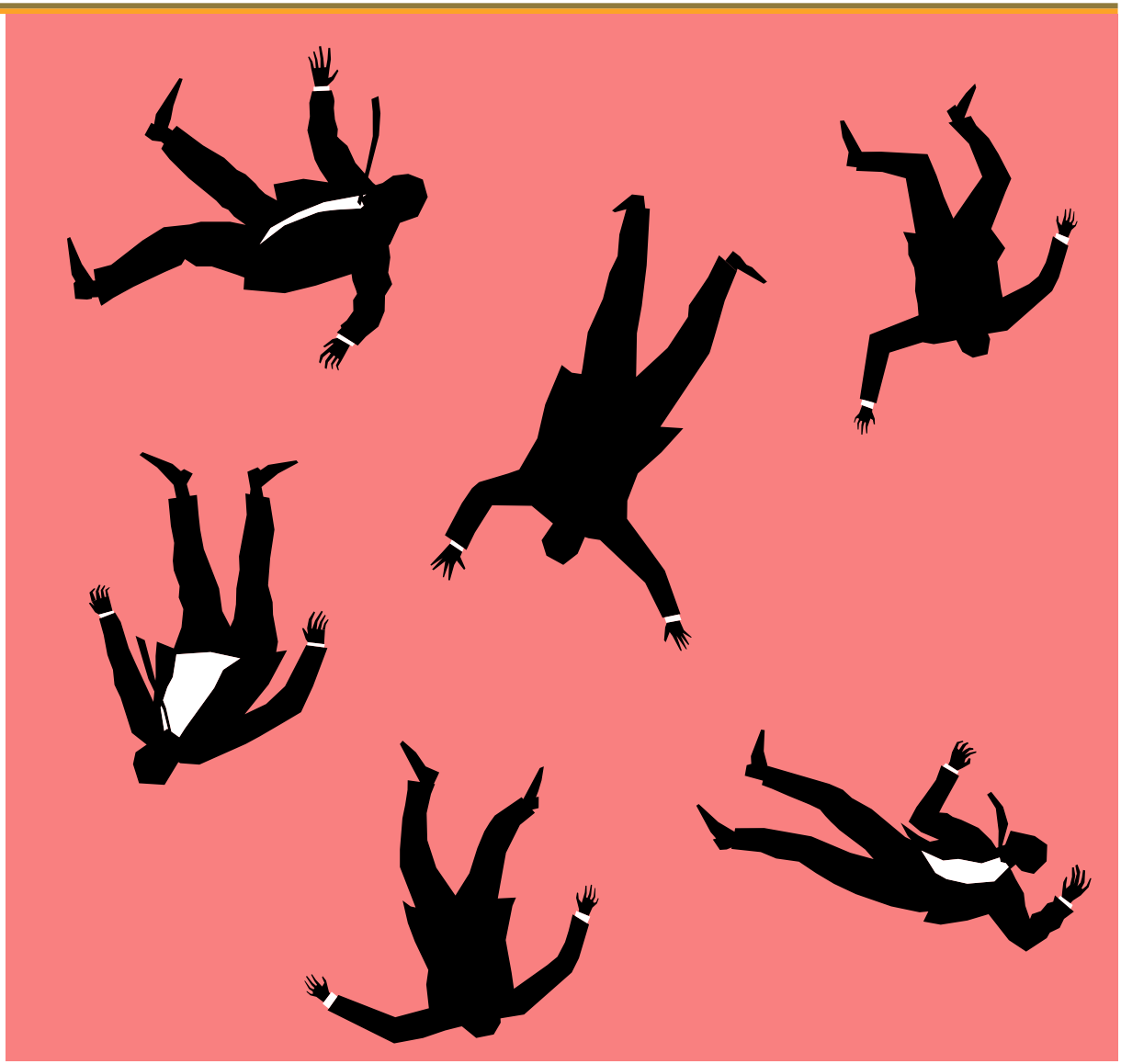
FOREWORD

Welcome to the forty-first issue of Risk & Compliance, an e-magazine dedicated to the latest developments in corporate risk management and regulatory compliance. Published quarterly by Financier Worldwide, Risk & Compliance draws on the experience and expertise of leading experts in the field to deliver insight on the myriad risks facing global companies, the insurance solutions available to mitigate them, and the in-house processes and controls companies must adopt to manage them.

In this issue we present features on creating a risk-intelligent organisation and on data breach management and response. We also look at: ESG and climate risk management; the future of data ethics and regulation; managing cyber risk in the energy sector; cyber security regulatory risk management; building a sustainable security and privacy programme; integrating risks into strategic decision making; the billion dollar rise of non-fungible tokens; the importance of a strong relationship between compliance and business teams; a 'pre and post' approach to compliance; the intersection between compliance and the arts; third party anti-bribery audits in the pharmaceutical sector; anti-corruption compliance and investigations in high-growth markets; and more.

Thanks go to our esteemed editorial partners for their valued contribution: SAS; and the Society of Corporate Compliance and Ethics (SCCE).

– Editor



Stay informed.

Wherever you do business, whatever your industry, you know the outlook can change in an instant. New risks emerge. Opportunities come and go. Preconceptions are overturned. To make sure you move with the times, get the information you need, when you need it.

Sign-up to receive the latest content from Financierworldwide.com, available on all your devices with a click or a tap. We'll send you essential notifications, along with access to password-protected pages for the latest news and analysis. It's quick, easy and free, so sign-up now and stay informed.

SIGN-UP FREE
www.financierworldwide.com

FINANCIER WORLDWIDE corporatefinanceintelligence

FEATURE

ANALYSING RISK: THE REWARDS OF INTELLIGENT RISK MANAGEMENT

BY **FRASER TENNANT**

Every organisation, regardless of its size and the sector in which it operates, faces risks. While many of these can be tackled effectively, the reality is that they cannot be eliminated entirely, rather managed and minimised to the furthest extent possible.

Moreover, risks are emerging at pace. In 2022, geopolitical tensions, the climate crisis, the after-effects of the global coronavirus (COVID-19) pandemic and cyber security threats all created a hugely challenging network of risks for organisations. Ramping these up considerably is the Russia-Ukraine conflict, which has sent shockwaves across the world.

Testifying to this is the World Economic Forum's (WEF's) 'Global Risks Report 2022', respondents to which said they expected the next three years to be characterised by either consistent volatility and multiple surprises or fractured trajectories that will separate relative winners and losers. Some foresaw progressive tipping points with increasingly catastrophic outcomes.

Adding further oversight as to the gravity of the current and future global risk landscape is the 'Munich Security Index 2022', which provides in-depth insights into how G7 and BRICS nations view 31 major global and domestic risks by combining five metrics: overall risk, potential damage, expected

trajectory, perceived imminence and feelings of preparedness.

The overall picture painted by the Index is one of growing concern about risk. Based on a survey conducted among 12,000 people globally, those polled indicated that they were more risk-aware than ever before. Moreover, in Europe and beyond, a sense of "collective helplessness" in the face of global events is prevalent.

"We live in a time of extraordinary uncertainty and turbulence," notes Vivek Prakash, chief consultant at pmwares. "Disasters, scandals and natural calamities are hitting enterprises, which highlights the importance of risk management at an enterprise level. Moreover, such events often raise questions as to the capability of executives and boards to foresee the unexpected.

"While a well-defined risk governance system may be in place and aggressively followed by board and management for financial risks, the same is not always true for other operational and strategic risks," he continues. "This is one of the main reasons why most risk strategies are not successful and often fail without delivering intended results."

Thus, while organisations may already have well-prepared infrastructure in place, behind the scenes, many still take a generally lax attitude toward risk awareness, a mindset which is likely to result in significant gaps and deficiencies in their risk posture.

Attitudes to risk

Risk attitude is the natural inclination or basic nature of an organisation's willingness to take a risk or not – a response driven by its perception of a given scenario – and to evaluate and respond across the enterprise.

However, a major hurdle with regard to achieving consistency in managing risk is that organisations, and the people therein, logically have distinct attitudes toward risks, and those attitudes will vary with circumstance.

According to Laevo's 'Defining Risk Attitudes' analysis, there are three distinct risk attitude types: risk aversion, risk seeking and risk neutral.

Risk aversion is a type of attitude where an individual inclines toward certain as opposed to uncertain events. A risk aversion type will leave a good chance of more profits on the table and look for a more certain scenario instead.

Risk seeking is a type of attitude or behaviour where someone gravitates toward uncertain activities in place of more certain ones. They display a risk-seeking attitude when they are ready to pay a penalty to take a risk.

Risk neutral describes an individual who possesses an indifferent attitude toward risk. They usually display their character when decisions are based exclusively on expected monetary value.

"Risk attitude can be defined as a chosen state of mind concerning those uncertainties that could have

a positive or negative effect on objectives," states Laevo. "Risk attitudes are generally implemented subconsciously and without mindful validation. However, like any other attitude, risk attitudes are a choice for an individual or organisation."

Ultimately, organisations must ask themselves some key questions. How much is their enterprise prepared for forthcoming risks? How can they identify the risk and take appropriate measures in time to prevent negative impacts? And how do they effectively link risk management to organisational strategy?

"A major hurdle with regard to achieving consistency in managing risk is that organisations, and the people therein, logically have distinct attitudes toward risks, and those attitudes will vary with circumstance."

Intelligent risk management

For virtually every organisation, day-to-day decision making across their entire enterprise is full of attendant risks. Thus, in order to recognise, quantify and ameliorate hazards, what is required is a way to systematically identify the impact and duration of risk incidents in a repeatable and verifiable way.

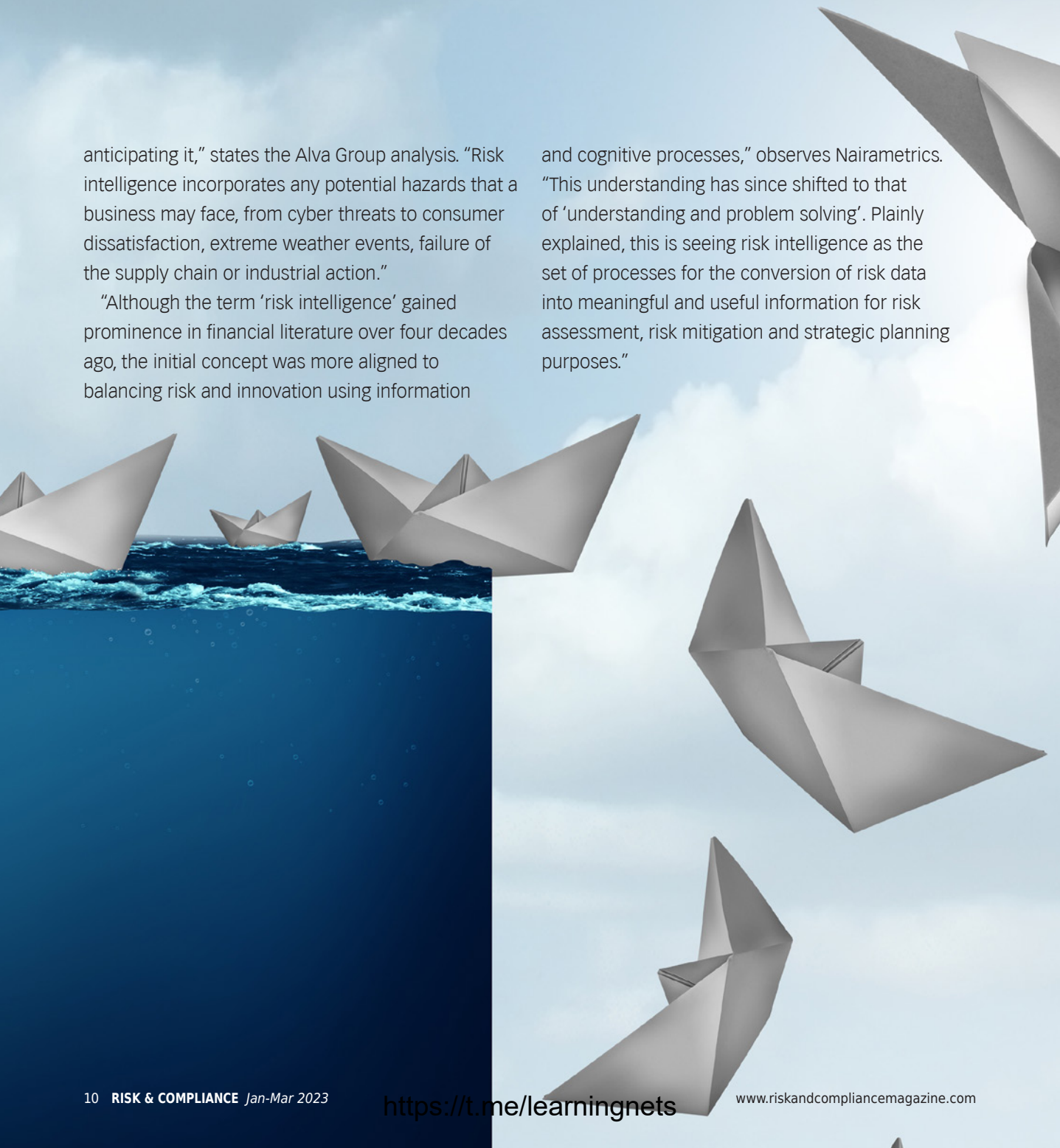
Enter risk intelligent enterprise management. As defined by Leo Tillman in his European Financial Review article 'Risk Intelligence: A Bedrock of Dynamism and Lasting Value Creation', risk intelligence is the organisational ability to think holistically about risk and uncertainty, speak a general common risk language, and effectively use forward looking risk concepts and tools in making better decisions, alleviating threats, capitalising on opportunities and creating lasting value.

Fleshing out the concept further is the Alva Group's 'What is Risk Intelligence' analysis, which states that risk intelligence enables organisations to systematically identify the impact and duration of stakeholder risk incidents in a repeatable and verifiable way. It also gives organisations the ability to gather information to identify and quantify risks – empowering them to make informed decisions about its risk exposure and security risks.

"Risk intelligence allows organisations to manage risk by identifying and alleviating threats, surfacing opportunities and, ultimately, create value for all stakeholders by moving from managing risk to

anticipating it," states the Alva Group analysis. "Risk intelligence incorporates any potential hazards that a business may face, from cyber threats to consumer dissatisfaction, extreme weather events, failure of the supply chain or industrial action."

"Although the term 'risk intelligence' gained prominence in financial literature over four decades ago, the initial concept was more aligned to balancing risk and innovation using information and cognitive processes," observes Nairametrics. "This understanding has since shifted to that of 'understanding and problem solving'. Plainly explained, this is seeing risk intelligence as the set of processes for the conversion of risk data into meaningful and useful information for risk assessment, risk mitigation and strategic planning purposes."



Building a risk intelligent enterprise

For many within the risk management fraternity, risk intelligence is the Holy Grail. It allows for strategic and day-to-day decisions to be made across an entire enterprise – a systematic approach to identifying, assessing and planning for risks, as well as making key risk information available at every organisational level.

According to the MetricStream report 'The Rewards of Risk Intelligence', for an organisation to become a risk intelligent enterprise, it needs to follow a number of steps, outlined below, to embed a thoughtful, sustainable consideration of risk into its key decision-making processes.

First, establish a specific process to uncover the poorly understood threats to the organisation. This should also be translated into common business terms to relate to the organisation's audience and stakeholders.

Second, bring key stakeholders together to address risks efficiently and sensibly. Whether they are the risk and control owners, or regulatory bodies, it is important to get their understanding of these risks and determine which emerging risks need greater focus.

Third, facilitate the drive for consensus among contributors on scenario planning, which is probably the best way to make possibilities real and to arrive at real strategies to counter possible negative impacts. However, driving a consensus on emerging risks is difficult because organisations could come up with multiple scenarios.

Fourth, review and eliminate, or defer low relevance risks. Because organisations are often grappling with resource constraints, efforts can be concentrated only on those risks that have relatively high relevance and probability.

Fifth, leverage emerging risk processes for competitive advantage. If organisations have an emerging risk process, they probably have by default some element of competitive advantage. That will be decreasingly so as more people realise this.

Finally, bring forward and highlight risks that lend themselves to exploitation. When looked at how risks can be turned into opportunity, emerging risks can present a means to grow and innovate.

"Being risk intelligent is probably the utopia for most organisations, as it quite often requires them to constantly determine their top risks and accordingly modify their risk management strategies," adds MetricStream. "Knowing what risks they can and should take, and what risks to keep at bay are vitally important to an organisation's health and value."

Another key aspect of an organisation's transition to becoming a more risk intelligent enterprise is the

role that culture has to play, and how this culture is disseminated by the board and senior management in particular.

"The practices and culture of an organisation percolate from the top," adds Mr Prakash. "Therefore, it is important that the board and senior management play a key role in fostering new approaches to risk oversight. The tone at the top sets forth the principles, values and ethical climate of an organisation. If the board and senior management uphold the importance of risk intelligence, the organisation will be more inclined to uphold the same values."

Modern risk management

In the face of growing geopolitical tensions and an increasing number of interlocking global crises, it is essential for organisations to solidify their risk awareness posture. The challenges of today's 'new normal' may be surmounted by embracing intelligence as a vital competitive tool.

"Organisations must confront challenges and ask questions about the continued relevance of their strategic vision, structure, business model competitive positioning and values in the new world order," contends Nairametrics. "The ability to innovate, remain competitive and sustain value creation in the 'new normal' will require a structured risk decision-making process that is both clearly predictive and robust."

For Mr Prakash, it is risk intelligence that can provide the answer to a host of risk-related conundrums. "Risk intelligent enterprise management considers risk as a key input into leadership decision making," he concludes. "It treats risk management as an integral part of the enterprise's strategy and operations and not as a separate process or discipline."

Ultimately, the harsh reality for organisations is that the decisions they take related to risk need to become increasingly savvy, with intelligent risk management proving, in real time, to be a game changer for the modern risk environment, in all its guises. R&C

FEATURE

DATA BREACH MANAGEMENT AND RESPONSE

BY **RICHARD SUMMERFIELD**

For all companies, the importance of being prepared for a data breach continues to rise. Cyber attacks can bring significant adverse consequences to an organisation. The level of readiness is likely to have a material bearing on the extent of the impact.

2021 was a record year for cyber attacks. In the US, the number of data breaches jumped 68 percent compared to 2020, reaching a level 23 percent higher than the previous all-time high, according to Identity Theft Resource Center (ITRC). A report by ProPublica reveals that 2021 saw the theft of 300 million customer service and device records from one company, 59 million email addresses and personal data from another company, and a 17.6-million row database from a third.

2022 has continued in the same vein. Data breaches in the first quarter of the year were up 14 percent over 2021, according to ITRC. That makes three consecutive years of Q1 increases. Stolen or compromised credentials were used to effect 19 percent of attacks, with phishing at 16 percent and cloud misconfiguration at 15 percent.

Between January and March 2022, there were 404 publicly reported data compromises, with phishing and ransomware attacks once again the most common types of intrusions. The healthcare, financial services, manufacturing, utilities and professional

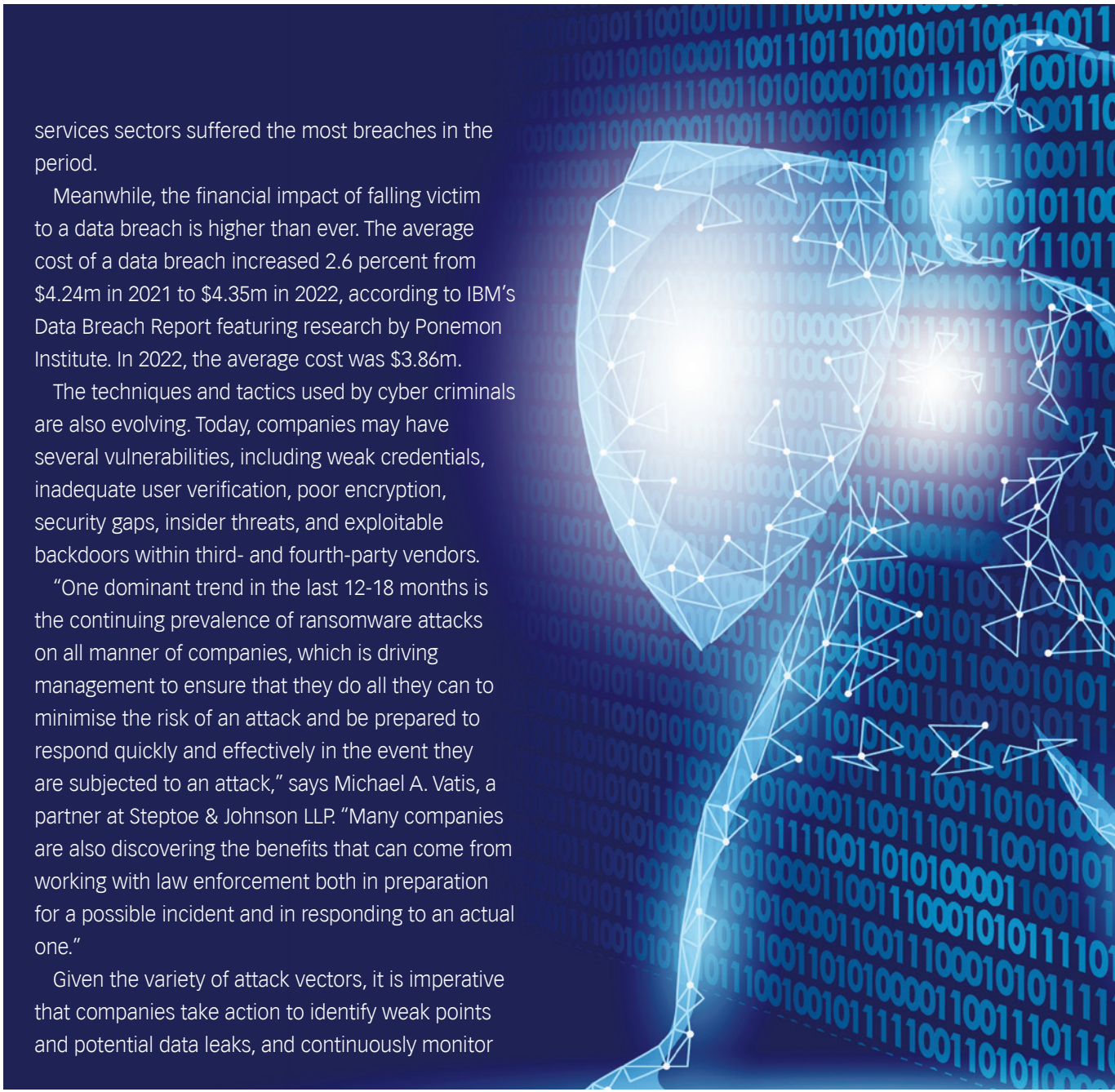
services sectors suffered the most breaches in the period.

Meanwhile, the financial impact of falling victim to a data breach is higher than ever. The average cost of a data breach increased 2.6 percent from $4.24m in 2021 to $4.35m in 2022, according to IBM's Data Breach Report featuring research by Ponemon Institute. In 2022, the average cost was $3.86m.

The techniques and tactics used by cyber criminals are also evolving. Today, companies may have several vulnerabilities, including weak credentials, inadequate user verification, poor encryption, security gaps, insider threats, and exploitable backdoors within third- and fourth-party vendors.

"One dominant trend in the last 12-18 months is the continuing prevalence of ransomware attacks on all manner of companies, which is driving management to ensure that they do all they can to minimise the risk of an attack and be prepared to respond quickly and effectively in the event they are subjected to an attack," says Michael A. Vatis, a partner at Steptoe & Johnson LLP. "Many companies are also discovering the benefits that can come from working with law enforcement both in preparation for a possible incident and in responding to an actual one."

Given the variety of attack vectors, it is imperative that companies take action to identify weak points and potential data leaks, and continuously monitor



their own security posture and that of their business partners.

Legislative developments

Against this backdrop is a tightening net of data privacy legislation. In the UK and continental Europe, for example, data privacy has generally been viewed as a fundamental human right. In other markets, such as the US, businesses must navigate a growing patchwork of state regulations. California, Colorado, Connecticut, Utah and Virginia all have their own consumer data privacy laws.

As Mr Vatis explains, a growing number of US states are enacting comprehensive privacy laws that give certain 'rights' to state residents with regard to personal information collected about them by private companies. This includes, for example, the rights to know what personal information has been collected, to delete it, to correct it, and to opt out of it being sold to or shared with other companies. "Each state law is slightly different, and so many companies are scrambling to be sure they will be in compliance with the five new laws, so far, that come into effect in 2023," he adds.

The laws have several provisions in common, such as the right to access and delete personal information and to opt-out of personal information being sold, among others. Other provisions require commercial websites or online services to post a privacy policy that describes the types of personal

information collected, what information is shared with third parties, and how consumers can request changes to certain information. By the end of 2023, 10 percent of US states will be covered by data privacy legislation, but the lack of a single federal law creates compliance complexity for companies operating in the US.

"The advent of new state privacy laws in the US is an important legal development that is affecting how companies store, use and share personal information about customers and other people they interact with," says Mr Vatis. "More and more states will be adopting such laws, creating a crazy quilt of varying requirements that companies will need to address. And unfortunately, there is still only a small chance of a federal law being passed in the near future that would pre-empt such state laws.

"In addition, we are already seeing in California, and will soon see in other states, state regulators beginning to enforce these new requirements," he continues. "Some of the consequences of these laws are that companies will need to have the ability to stop sharing or 'selling' data when so requested by consumers, or to delete or correct information. And they will need internal processes to respond to consumer requests. In addition, both federal and state legislators and regulators are putting renewed focus on protecting the privacy of children, which will complicate data handling by companies."

According to Gartner, the personal data of 65 percent of the world's population will be protected by modern privacy regulations by 2023 – a major jump from just 10 percent in 2020. Complying with these expanding regulations is challenging for companies, but necessary to avoid negative financial and reputational repercussions.

Part of achieving compliance with data privacy legislation is ensuring that data protection initiatives and data governance programmes are established in a holistic way, providing clear visibility into a company's regulated and sensitive data. Working with trusted business and technology partners who understand the data privacy space can help companies adapt to rapidly evolving regulations.

Response planning

How companies respond in the event of a breach is critical. Certain step must be taken to regain the trust of stakeholders. But organisations are often found to be lacking in certain areas. Data breach reporting, for example, remains inconsistent at best, according to ITRC.

With growing regulatory and stakeholder expectations, it is critical that companies put in place a data breach response plan. "Many companies have finally moved out of the 'oh, breaches happen to other people' stage and understand that data breaches are all too common and perhaps even unavoidable," suggests Mr Vatis. "But many

companies still do not have an operational breach response plan in place.

"There are key features of an effective plan," he continues. "First, draw up a list of the roles and responsibilities of each key player who will need to be involved in a breach response. Second, make prior arrangements with, or at the very least have contact information for, vital outside actors who might need to be engaged during a response, including outside counsel, a forensic investigation firm, public relations advisers, and law enforcement personnel. Lastly, draft an outline or checklist of potential urgent actions to be taken to minimise damage and loss."

Once a plan has been drafted, it then needs to communicated, understood by key individuals, and regularly tested. "At least as important as the plan itself is rehearsing the response as part of a tabletop or 'live' exercise," says Mr Vatis. "Create realistic scenarios and then run through them with key executives so that they have a better, more visceral understanding of what an incident will feel like, where gaps may exist in their planning, and what each person's responsibilities are. Practice does not make perfect, but it does make a real-world response much more likely to be effective."

Should a successful attack occur, companies must move quickly to contain the breach and mitigate its effects. The first step is to activate the incident response plan. An effective and timely response plan can minimise the impact, soften any negative press, reduce the potential of a regulatory fine, and help get the company get back to business as quickly as possible.

"Breach response is hugely important; it cannot be treated as a mere box-ticking exercise. For a response plan to be effective, it must also have the backing of the company's senior management."

Part of the response plan will include establishing an incident response team with the skills and experience to deal with a data breach. The team should utilise incident managers, digital forensics experts, malware analysts and security operations centre (SOC) analysts. They will need to make key decisions, conduct an in-depth investigation, provide feedback to stakeholders, and provide assurances

to senior management that the situation is under control.

To coordinate the process, companies should establish clear lines of communication immediately following a breach. Those individuals and groups responsible for sending out correspondence, assigning tasks and taking appropriate action should be clearly set out in the response plan and know exactly what is expected of them.

Breach response is hugely important; it cannot be treated as a mere box-ticking exercise. For a response plan to be effective, it must also have the backing of the company's senior management.

Not only is an effective data breach response plan prudent from a financial and reputational perspective, there is often also a legal responsibility. Data privacy regulations, many of which have been built on the European Union's (EU's) General Data Protection Regulation (GDPR), typically specify how an organisation must respond upon learning of an attack.

To that end, the response should adhere to reporting requirements mandated in jurisdictions where the company operates. The GDPR, for example, introduced a requirement for organisations to report personal data breaches to the relevant supervisory authority, if the breach presents a risk to the affected individuals. Organisations must do this within 72 hours of becoming aware of the attack.

For companies that may find it challenging to create and implement a successful response plan, there are guidelines and templates available to help, such as those of the UK's National Cyber Security Centre (NCSC).

Lastly, the fallout from a data breach can be painful and expensive, but companies should not overlook the opportunity to learn valuable lessons. Once a breach has been contained and systems have been brought back online, the response team should complete a focused internal evaluation and review the events of the breach to understand what could be done better.

That way, the company can improve its preparations for the next attack. R&C

EXPERT FORUM

ESG AND CLIMATE RISK MANAGEMENT: THE ROAD FROM COMPLIANCE TO OPPORTUNITIES

PANEL EXPERTS

Giada Scalpelli
Senior Customer Advisor Risk Management
SAS
T: +39 345 544 9185
E: giada.scalpelli@sas.com

Giada Scalpelli is part of the customer advisory risk management team at SAS Italy. In this role, she helps clients deal with the many challenges of credit risk topics, such as IFRS9, stress testing and regulatory capital. Before joining SAS and after a long period abroad, during which she studied at Universiteit Leiden and at CWI, the national research centre for mathematics and informatics in the Netherlands, she graduated in mathematics at Università degli Studi di Padova.

Ahmet Cenk
Senior Risk Management Advisor
SAS
T: +971 56 175 7560
E: ahmet.cenk@sas.com

Ahmet Cenk is working as a senior engineer and expert consultant in various projects in the fields of risk management, risk reporting and risk modelling. He has been working in the Middle East, Turkey and Africa region in the last four years. He worked on various risk fields including credit, market, ALM, regulatory modelling and recently focused on sustainability and ESG risk management. He is member of the ESG team operating in EMEA and APAC

Pablo Chong
Risk Solutions Advisor
SAS
T: +852 9855 3120
E: pablo.chong@sas.com

Pablo Chong has a decade of experience in risk management, including top lending institutions in both LATAM and APAC markets. He has covered different areas in credit risk such as model development and monitoring, scorecards, regulatory capital and pricing parameters (largest bank in Peru), strategy development, portfolio management and implementation (APAC portfolio), model validation (wholesale – global models) and decision systems (Hong Kong portfolio). He also understands the importance of climate risk in risk management and has recently passed GARP's SCR certification.

R&C: Could you provide an overview of recent trends around environmental, social and governance (ESG) and climate related risks, regulations and opportunities? Are you seeing these issues ascend to the top of the corporate agenda?

Cenk: A central strategy around sustainability is one of the top agenda items for a range of corporates, including financial services. As the world is going through turbulent times from an economic, climate, political and social perspective, building robust businesses that are sustainable in the long term should be a central criterion for all decisions. Increasing sustainability is perhaps the most important aim of the environmental, social and governance (ESG) related regulations which have been introduced in recent years, and we expect more regulations to guide corporations in this direction. It is also encouraging to see the consolidation work being carried out by the International Sustainability Standards Board (ISSB) and other regional authorities around sustainability-related disclosures. The recent publication of the European Union (EU) Corporate Sustainability Reporting Directive (CSDR) is a further example of the intensification of regulation to disclose more on ESG-related matters.

Scalpelli: The world is increasingly focused on ESG issues, as well as on climate change related risks. Furthermore, there is increased attention being paid to climate change by regulators, banks and the wider business community. There are different reasons for this heightened interest. First, climate change related risks are becoming more material and have the potential to impact companies' financial performance. Second, there is a growing recognition that these risks need to be managed in a proactive and holistic manner, integrating them into companies as 'business as usual' (BAU). And finally, there is an increasing awareness of the opportunities that can be generated by addressing these risks and vulnerabilities. In response to this growing awareness, several initiatives have been launched in recent years to promote greater disclosure of information on companies' exposure to climate change risk. The European Central Bank (ECB) launched the first EU-wide climate stress testing exercise at the beginning of 2022, and the results published in the summer made the ECB position clear that banks must sharpen their focus on climate risk. In fact, the stress test showed that credit and market losses amount to around €70bn on aggregate for the 41 banks tested. But, according to the ECB, this significantly underestimates the actual climate-related risk. In the coming years, exercises of this kind are going to become more frequent, with the final goal likely to involve climate risk being

considered in the same manner as credit, market, operational and liquidity risk.

Chong: Regarding opportunities around climate-related risks, both physical and transition risks can offer favourable outcomes. Companies exposed to physical hazards need to invest significant amounts to protect their facilities and prevent large-scale losses. While there is an expectation that preventive activities do not create revenue streams per se, there is an opportunity for companies to partner with governments and be rewarded for their operations in industries or areas exposed to physical hazards. Another example is cooperation between companies and communities, such as building adaptive infrastructure to protect both facilities and their surrounding areas. Regarding transition risk, opportunities will be more likely for more agile firms. For instance, as consumers increase their awareness of the climate impact of their purchases, flexible firms will offer a larger set of sustainable products, while other firms will be left behind.

R&C: In what ways has recent turbulence around the world accelerated ESG ambitions? What role have specific events played in this uptick?

Cenk: Although the recent challenges the world has faced pushed many to the limits, we cannot deny that there have been some upsides. For example, the coronavirus (COVID-19) pandemic led to the increased adoption of virtual meetings and events. Before the pandemic, large groups of professionals were used to physically coming together to discuss issues that could have been discussed more efficiently online. The pandemic and subsequent lockdowns made the switch to virtual meetings necessary, and similar changes have happened in other areas of daily life. We are seeing more companies adopting energy efficient methods after seeing the success of making such changes the 'new normal'. Organisations are increasingly adopting hybrid work that helps to reduce the emissions generated by employees commuting. Equally, we are seeing organisations adopting paperless and contactless policies that help to reduce consumption of limited resources.

Scalpelli: In addition to recent climate-related turbulence, global conferences, like COP27, and agreements between nations around the world are accelerating climate action. Furthermore, as the world progresses toward the goals set out in the Paris Agreement, the banking sector will need to play a key role in achieving a net-zero future. Many banks are already starting to act on climate change, with several organisations committing to net zero strategies and goals. This is a welcome development,

as the banking sector has a critical role to play in financing the transition to a low-carbon economy.

Chong: The increasing frequency of weather-related events, such as extreme heat, droughts and floods, has caused major disruption around the world. These kinds of acute physical hazards can create abrupt losses to corporations, such as floods triggering collateral depreciation. In addition, severe physical hazards, such as rising sea levels, can also generate negative effects like coastal flooding risk. Research suggests properties exposed to rising sea levels tend to sell at a discounted price on average compared to unexposed properties. In this context, and with more frequent physical risks expected in the future, corporations and financial institutions (FIs) have started to take environmental matters much more seriously, not only because they can constrain business performance, but also because human action is very likely the main reason for recent global warming, according to the Intergovernmental Panel on Climate Change (IPCC).

R&C: What are the main challenges for teams involved in ESG and climate risk management? How is technology helping in this area?

Cenk: There are many challenges for sustainability teams. First, the lack of concrete, consolidated and unified methodology to measure certain indicators is causing teams to be particularly cautious. The landscape is evolving so quickly, regulators, practitioners, consultants and the general public are finding it difficult to keep up to date. This is causing organisations to diverge from their own path, reducing timelines and chances to sync. Taking care of the environment is a collaborative task and lack of unified guidelines is a concern. The greatest allies companies can have are agile and flexible digital tools that will help organisations keep themselves up to date and sync with each other on the methods and data that they use in a structured manner. Deploying analytical tools and leveraging them to

> **"As with any analytical tool, data is a key input. In that sense, understanding novel data sources, like climate data, is one of the main challenges for risk managers."**
>
> *Pablo Chong, SAS*

make data driven agile decisions is the best step companies can take to cope with the ever-changing dynamic nature of the landscape.

Scalpelli: Climate risk management is the process of identifying, assessing and responding to climate risks. It is a critical component of climate change adaptation and mitigation. Climate risks include both transition risks, posed by the economic shift toward a sustainable future, and physical risks, posed by extreme weather events and as a direct consequence of climate change. Therefore, given its nature, climate risk management poses some complex challenges. First, it is necessary to integrate climate scenarios for physical and transition risks. These scenarios are long-term scenarios, with impacts over decades, not years. Furthermore, if the goal is to analyse the most remote future, it becomes fundamental to have a dynamic portfolio integrating the impacts of possible green or net-zero strategies, or changes in climate policies. Finally, regarding models, the transmission channels, which represent the connection between classic risk parameters and climatic variables, is the main challenge FIs are facing. Technology can help climate risk management with a dynamic, scalable and integrated platform that is flexible enough to allow management of different types of scenarios and strategies, providing an integrated platform for regulatory and strategic simulations.

Chong: In risk management, it is common practice in the banking industry to use technology and analytical tools. For example, credit risk managers use scorecards to assess credit applications and manage their portfolio, among other use cases. As with any analytical tool, data is a key input. In that sense, understanding novel data sources, like climate data, is one of the main challenges for risk managers. Fortunately, technology can help in this endeavour, for example by analysing physical hazards and visualising them with portfolio data at different granularity levels, or using scenario analysis tools to examine exposure to sectors highly exposed to

> **"Although the recent challenges the world has faced pushed many to the limits, we cannot deny that there have been some upsides."**
>
> *Ahmet Cenk, SAS*

transition risk, using the Network for Greening the Financial System (NGFS), IPCC or other scenarios.

R&C: How can banks and corporates build a strong foundation for ESG and climate risk impacted systems? Can this be embedded into business as usual (BAU)?

Cenk: To build a strong foundation, organisations must address the right problem with the right solution. The biggest challenge that organisations can solve internally is the process of collecting ESG data. Lack of data is one of the biggest challenges in this area which prevents disclosure of useful information to both internal and external stakeholders and may eventually cause big impact incidents. Some of the largest entities are calling ESG the most data-intensive exercise of their lives. As this is a universal problem, waiting for a solution from vendors, consultants or government organisations is not preferable, and doing so will put organisations at a disadvantage. The analytical systems that allow organisations to collect granular data at individual asset level, at third-party level, at department level and at product level, on a monthly or even daily basis, are better able to analyse the situation and provide insights for optimisation sooner. Furthermore, organisations also need governance around the process, so that the data and the decisions made are held to account. Analytical systems adopted by entire organisations provide a strong foundation and embed this approach into their day-to-day operations.

Scalpelli: When it comes to climate change risks, banks need to have a clear understanding of the potential impacts of climate change on their business, and climate stress testing is a fundamental tool at their disposal. Regulators agree that building a strong climate stress testing platform is the first step toward managing climate risk. According to the results of the ECB Climate Stress Test exercise, banks currently fall short of best practices, and should establish climate stress testing capabilities that include several climate risk transmission channels and portfolios. Climate stress testing can and must be integrated into BAU activities, leveraging what has already been built for traditional stress testing exercises. Firms should seize this opportunity to review the structure of current processes, which are often handled with customised tools.

Chong: Novel data sources like climate data need to be properly understood before they can be embedded into BAU, especially given the lack of standardisation and overall experience with its application to risk management. A gradual approach should be adopted. For instance, climate-related data can initially be used to gain a better understanding of portfolio exposure to physical hazards. Once business

owners and risk managers understand the basic relationships between their portfolio and climate-related data, they can progressively incorporate this into credit risk policies. At a later stage, the impact of physical hazards can be tested in credit risk models.

R&C: Given that ESG is a broad, constantly evolving field, what concrete steps should companies focus on for risk management and compliance?

Cenk: ESG is a broad subject touching upon myriad areas of a business, from environmental impact to social conduct, from decarbonisation projects to setting proper oversight, from employee empowerment to supply chain integrity. Building a sustainable future, planet and business requires improvement in all these areas, which is challenging from many perspectives. One challenging aspect, and an initial step to improve matters, is the ability of parties to measure and quantify ESG. Organisations need to understand ESG areas and build robust frameworks to measure them, which will allow quantification of ongoing risks and opportunities. This measurement should also consider the data generated throughout the process and ensure it has the right granularity and frequency to make it useful for the decision-making process.

Scalpelli: When we talk about ESG and climate risk we are talking about a wide range of topics, including challenges and opportunities, each of which has its own peculiarities which must be addressed with a common sustainable strategy on the one hand, and with specific tools on the other. If we focus on climate risk, regulators have been paving the way for FIs to develop their own methodology and approaches. There are different ways that banks can use climate stress testing to gain insights into how climate change may impact their business. For example, banks can use climate stress testing to identify which business activities are most vulnerable to climate-related risks and assess the financial impacts of climate change on different parts of the bank's business, to determine the resilience of the bank's operations and infrastructure to climate-related risks and to develop strategies for managing and mitigating climate-related risks. By gaining insights into how climate change may impact their business, banks can make informed decisions about how to best protect their business.

Chong: As chief risks officers (CROs) have noted, if you peel back the layers of climate risk, the complexities are enormous. With respect to retail banking, companies are reacting to pressures and shifting their business models, which eventually impacts individuals. It is not a direct connection; rather, there are second- and third-degree impacts,

which makes modelling incredibly complicated. You cannot worry about the things you do not know. It is things that banks have no real experience with that keep them up at night.

R&C: Is there potential to gain added business value from effective ESG management? What benefits may be derived?

Cenk: One of the prevailing reasons corporates are investing in ESG management is to collect, measure and disclose more information related to the business benefits it brings, rather than to merely achieve compliance with regulations. There are many studies analysing the relationship between ESG investments and rating, and financial performance. The results are rather decisive, demonstrating that companies that invest more to achieve effective ESG management and disclosure outperform their competitors in key performance indicators, such as revenue, growth and equity price. This is mainly driven by consumers whose awareness around environment and social matters has grown tremendously in recent years. There is an increasing loyalty and willingness among consumers to pay a premium for more sustainable products and services. However, it is important to mention that we should look for truly sustainable ways of doing business in order to tap into such opportunities and not jump to short-term benefits.

Scalpelli: By identifying and assessing climate risks, both physical and transition, local authorities and the wider economy can create more awareness on climate change and develop plans and strategies to mitigate and adapt to the effects of climate change. This will help to improve resilience and reduce the potential impacts of climate change on businesses, infrastructure and communities. FIs can play an important role in climate change mitigation by financing projects and initiatives that help to reduce greenhouse gas emissions. By doing so, banks can help to promote the transition to a low-carbon economy and support the goals of the Paris

> **"Climate stress testing can and must be integrated into BAU activities, leveraging what has already been built for traditional stress testing exercises."**
>
> *Giada Scalpelli, SAS*

Agreement on climate change, as well as supporting their clients and employees in making more sustainable choices. From a business perspective, banks can seize the opportunities arising from this societal shift, but only with effective management of climate-related risks which allows the impacts of different local and international green policies under their sustainable strategies and net-zero commitments to be assessed.

Chong: Benefits can be derived from opportunities around climate-related risks. In terms of physical risks, collaboration between companies, governments and local communities is required, as there are industries naturally exposed to physical hazards. Without collaboration, physical climate risks would become a burden for governments. On the other hand, long-term benefits for companies and FIs can be achieved if all parties work together. A good example is the proliferation of sustainable finance, which involves any kind of financial activity that takes sustainability into account, such as the issuance of green bonds ring-fenced for environmental projects, or banks offering sustainability-linked loans where interest rates are linked to a company meeting certain sustainability benchmarks. Transparency in credit decisioning remains a big issue, even without the overlay of ESG factors. Customers will need help to understand the impact of their choice over the full term of any loans they take on.

R&C: From a regulatory and market perspective, what is the outlook for sustainability? What advice would you offer to companies on drawing up a sustainability roadmap?

Cenk: We believe stakeholders in this area have formed a consensus on the outlook for sustainability, which is becoming much more stringently regulated by global bodies and national organisations alike, as demonstrated by the COP27 event in Egypt. Consolidation work is being undertaken by the ISSB. A carbon tax levied on companies importing goods into the EU will come into effect in 2023 for certain sectors before a wider rollout for all industries. The EU's CSDR for corporates and small- to medium-sized enterprises (SMEs) within the EU has also been finalised. Going forward, organisations will likely become stratified based on their compliance with these regulations. Organisations with more agile, digital, transparent and comprehensive approaches to managing ESG are likely to cope better, and in a more practical way that helps with compliance as well as tapping opportunities.

Scalpelli: We live in an ever-changing world where exceptional events have become the new normal. Climate change is one of these events and the impact it might have in the coming years will depend on actions the world takes today. This is the

reason why ESG and climate risk is the number one item on market and regulatory agendas. The direction of travel is clear: banks must include climate risk management in their BAU processes, using it as an opportunity to modernise their overall approach. As Albert Einstein said, the measure of intelligence is the ability to change. And the only way to deal with the changes that surround us is by changing with them, so banks will also have to innovate their processes and approaches, transforming themselves to seize the opportunities associated with the ecological transition. R&C

PERSPECTIVES

THE FUTURE OF DATA ETHICS AND REGULATION

BY **ROBERT BOND**
> SCCE & HCCA

The Oxford Dictionary defines regulate to mean "control by rule" and defines regulation to mean "the imposition by government of controls over the decisions of individuals or firms". We have to ask ourselves, in relation to the regulation of data, what exactly we should regulate? Should we regulate the carriers that are responsible for the infrastructure over which data is disseminated, should we regulate the content providers who develop the data content that is disseminated, or should we regulate the data itself?

Over 20 years ago, a Ditchley conference in the UK on the regulation of cyber space concluded: "Regulations should be reflective rather than reactive. Regulations should control that which is bad and support that which is good. Regulations should be introduced on an international basis whilst acknowledging cultural and social individualities of nations and communities."

Data knows no jurisdictional boundaries nor restrictions on international data transfers, and so it seems odd that in 2022 we are still debating regulations that seek to control transfers of personal data. We should have reached a point in time where the need to respect personal information, keep data secure and enable trust becomes not only a focus for regulators and an expectation for citizens, but

also a compliance and ethical duty for governments and businesses.

Governments and other authorities have for thousands of years collected information on citizens in a variety of ways, and statistical information about people has been a valuable tool for managing economies and humanitarian needs. More recently, however, technological advances have meant that personal data can be collected, obtained, analysed, used, transferred and shared in myriad ways – some good and some bad.

We have certainly reached a point in time where personal information has a tradable value, but the trading in such data comes with moral and ethical obligations as well as legal and regulatory requirements.

As consumers become more educated about the ways in which their personal information is collected and shared, and how the appropriate use of such data can provide valuable outcomes, so consumers also expect legal and ethical standards to be adhered to. Where rights in personal data are abused and where such personal data is used for purposes for which consumers have no reasonable expectation, consumers will exercise their rights both legal and moral to gain satisfaction and compensation for failure by governments and

businesses to respect privacy, secure data and enable trust.

The notion of protecting personal data and rights in personal information has been around for hundreds of years as demonstrated by the right to "private life" in the French Constitution of 1791, the notion that "the individual shall have full protection in person and in property" as developed by Samuel Warren and Louis Brandies in 'The Right to Privacy' published in 1890, and the specific laws around the protection of personal data established in Europe since the Land of Hesse Act 1970.

More recently, the European Union (EU) General Data Protection Regulation (GDPR), which came into force on 25 May 2018, established a framework designed to support the processing of personal data while imposing on data controllers and data processors, both within government and industry, duties of transparency, fairness and accountability. Many global data privacy laws are based on principles laid down by the Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines and Convention 108, as well as the historic influence of Europe in its former colonial territories in the Americas, Africa, Middle East and Asia.

Recent well-publicised data breaches have demonstrated that the failure to respect privacy and to keep data secure has a direct impact on trust. Consumers are exercising their rights and demonstrating their expectations by choosing to engage only with businesses that demonstrate trust and integrity when processing personal data and avoiding businesses that plainly do not. The financial markets also react to data breaches, which has an impact on shareholder value. Corporates are now directly responsible to their shareholders for failures to keep personal data secure, and in addition regulators are taking an increasingly tough stance on those that fail to manage information securely.

"We have certainly reached a point in time where personal information has a tradable value, but the trading in such data comes with moral and ethical obligations as well as legal and regulatory requirements."

Regulations are dependent upon the way in which individuals observe them. In his paper 'Ethics in Business Practice and Regulation', Christopher Hodges says: "Research into behavioural psychology

has identified a number of important findings on why people observe or break rules. We now know many reasons why people may fail to observe a rule, notably because of inertia, procrastination, the influence of others especially social groups, mis-framing of issues, mistakes in assessing probability, not knowing exactly what to do, and so on."

Decisions are made by people rather than by organisations, although the structures, systems, objectives, culture and incentives that operate within organisations can affect the decisions made by the people who work in them. The focus of achieving compliance with laws should, therefore, be on affecting both the behaviour of individuals and the organisational environment.

The essential findings of the behavioural research are that people obey rules where: (i) the rule corresponds to their internal moral value system; (ii) the rule has been made fairly; and (iii) the rule is applied fairly.

Each one of these findings is based on the concept of fairness. In other words, ethics is central to people's observance of rules, and an advanced contemporary society that seeks to maximise compliance with its rules cannot avoid basing both the substance of its rules and the way they are made and applied on the sound ethical principles that are followed by that society. Basing regulatory and compliance systems on ethical norms and practice will, therefore, be essential for success. Equally, where actions are driven by dishonest, unscrupulous or wilful motives, the identification of such actions and the imposition of meaningful and proportionate sanctions is required.

Thus, it will be important to align the ethical values of individuals, work groups and businesses with those of the wider society in which they exist. Reaching and maintaining consensus on what the society regards as ethical gives rise to a need for ethical education, and ongoing discussions, reminders and checks. The substance of the 'rules of the game' should be agreed as being fair, expressing the essential values of the society. Making rules by a fair procedure will mean requiring fully enfranchised involvement, open and predictable processes, full notice of proposals and adequate opportunities for public consultation, analysis and debate before decisions are made. Applying rules fairly will mean ensuring that that wrongdoing is identified, and that responses to wrongdoing are applied proportionately, fairly and consistently.

The OECD's 'Good Practice Principles for Data Ethics in the Public Sector' guidelines state the following.

First, data ethical frameworks do not replace, but rather complement, support and are interconnected with relevant hard law instruments such as regulations on privacy, data protection, open data, open government, transparency and data sharing within the public sector, among others.

Second, the publication of and adherence to non-binding guidelines or standards such as the 'Good Practice Principles' do not guarantee real-world implementation. The effective alignment with and success of data ethical frameworks require their incorporation into public sector decision-making processes and the articulation of specific actions at a more granular and technical level (e.g., data management rules).

Finally, the effectiveness of data ethical frameworks is not achieved in isolation. Putting in place sound data governance arrangements in the public sector (e.g., institutional roles and responsibilities, coordination fora, advisory bodies and accountability mechanisms) is a precondition for success.

The use of new technologies such as smart devices, internet of things and artificial intelligence, coupled with the economic and humanitarian uses of big data analytics, means that there has to be a balance between the acquisition of personal data and the rights of citizens.

A balance has to be struck between the needs of governments to access personal data, the economic drivers for businesses to process and share personal data, and the rights and expectations of citizens in the control of their personal information. Governments need to implement laws and regulations that appropriately manage the data ecosystem and be accountable for their own use and misuse of personal data. And they must encourage education and communication to both businesses and citizens as to the duties and standards that attach to economic and ethical use of personal data. R&C

Robert Bond
Immediate Past President
SCCE & HCCA
T: +44 (0)7880 892 717
E: rtjbond@icloud.com

ONE-ON-ONE INTERVIEW

MANAGING CYBER RISK IN THE ENERGY SECTOR

Leo Simonovich
Vice President and Global Head, Industrial Cyber and Digital Security
Siemens
E: leo.simonovich@siemens-energy.com

Leo Simonovich is the vice president and global head of industrial cyber and digital security at Siemens Energy. He is responsible for setting the strategic direction for Siemens' industrial cyber security business worldwide. He identifies emerging market trends, works with customers and Siemens businesses to provide best-in-class cyber offers, and contributes to the company's thought leadership on the topic. He is particularly focused on solving the cyber security challenge in the oil & gas and power sectors by bringing unique solutions to customers looking to address a growing and costly operational security risk.

R&C: To what extent are companies in the energy sector especially vulnerable to cyber attacks? What makes them particularly attractive targets for malicious actors?

Simonovich: Attacks against the energy sector are frequent and sophisticated. The energy sector is increasingly digitalised, with physical equipment and IT systems now more interconnected than ever before. Optimising for low emissions and for low costs both require digital management of physical assets. Powerful efficiencies result from this digitalisation, but so do attack pathways. Energy infrastructure makes an attractive target because it is high value, both in terms of financial value, and in terms of geopolitical value. Some attackers are looking for financial gain, but some are backed by governments with geopolitical goals. In both cases, energy sector companies are appealing targets.

R&C: What types of cyber attacks seem to appear more frequently within the energy sector? To what extent do different types of attack require different risk management strategies?

Simonovich: Companies in the energy sector need stronger monitoring and detection capabilities than some other sectors, for a number of reasons. First, we are seeing attacks in the energy sector which are designed to compromise infrastructure for later disruption. Attacks are designed to give outsiders the ability to stop or disrupt operations at will. This is a very desirable type of attack for a foreign government. Infrastructure operators should develop capabilities that can detect such attacks in their initial stages and before any damage or disruption occurs. Second, attacks on IT can have consequences for physical equipment. Energy sector companies must be able to confirm that physical equipment is unaffected and safe to operate and must understand how their IT and operational technology (OT) equipment is integrated. As we saw

"Energy infrastructure makes an attractive target because it is high value, both in terms of financial value, and in terms of geopolitical value."

Leo Simonovich, Siemens

with the Colonial Pipeline, a ransomware attack in one part of an organisation can have cascading consequences; a company might be entirely unable to operate or might be able to deliver fuel but be unable to bill for it. Finally, the energy sector is a tightly networked supply chain. In the electricity business, cascading consequences can propagate at the speed of light. Mitigation must occur at machine-like speed.

R&C: How would you characterise the risks of a cyber attack arising from an internal versus an external source? How important is for energy companies to be vigilant and enhance their controls and defences on both fronts?

Simonovich: In the energy sector it is reasonable to assume that an external attack will also try to move laterally after breaching defences. In that sense, internal and external threats are not strictly different. Energy companies must be able to recognise malicious behaviours and commands that originate from authorised users and devices. Unlike IT, where attacks may come with distinctive signals like increased network activity or signatures in lines of code, attacks on the energy sector can be made with valid commands in an inappropriate context – for example, telling a turbine to spin and stop quickly to shake it apart. It is important to be able to recognise malicious activities, no matter where they originate.

R&C: What advice would you offer to energy companies on assessing and understanding the cyber risks and exposures they face, so they can develop adequate defences?

Simonovich: First, plan for change. Threats are constantly evolving. Every company can improve its cyber security maturity and risk management. Cyber hygiene is a basic but often lacking step. That means things like two-factor authentication, and training employees on how to avoid common attacks. For companies that are more mature, thinking through how to assess threats and prioritise responding to alerts is critical. Companies should be able to quickly determine which threats will be consequential for their business processes and focus on those threats. Automating routine tasks to free up time for cyber security analysts to actively hunt for threats is a good idea. One common point of failure is alert fatigue. This happens when defenders see so many alerts that the signals of actual attacks get lost in the noise of false positives. Cyber security also reaches beyond individual companies. We can strengthen each link in the value chain and help make the whole ecosystem more secure. Participate in information sharing efforts. Reach out to government counterparts to

establish contacts before an incident occurs. Talk to your suppliers and key partners about their cyber security efforts and response plans.

R&C: In the event of a cyber attack, what initial steps should a company take in response, to mitigate and contain the damage?

Simonovich: When an event occurs, defenders must identify which systems are involved. Understanding the nature of the threat and the likely goals of the attacker may enable defenders to block further damage and will give decision makers the best information possible to take further action. Where monitoring is unavailable, brute-force actions like total shutdown may be necessary. Defenders will want to contain the attack fully while minimising disruption on production. Once the attack is contained, defenders can work to eradicate the threat and restore functions. Responses are best with advanced preparation. That includes monitoring and detection capabilities, as well as a playbook that will guide responses, and running exercises to test how planned responses will work, then learning from those experiences. Playbooks need periodic updates to ensure that contacts, phone numbers and so on, remain current. During and after attacks, companies should share threat information to the extent possible. Sharing information across the industry can blunt attacks, making them less effective and less profitable for attackers.

R&C: What role can cyber insurance play in mitigating or transferring risk for energy companies? What considerations should be made when evaluating policy options and coverage on offer?

Simonovich: Estimating the financial risk associated with cyber attacks is still very challenging. Companies should work to assess their own vulnerabilities and level of risk. They should be thinking about whether they will emphasise buying down risk through insurance or through building cyber defence capabilities. Companies should also consider the reputational risks that come with outages caused by cyber attacks. Cyber security is a key enabler for reliable delivery of energy.

R&C: How do you expect the cyber risk landscape to evolve in the months and years ahead? How can energy companies ensure they remain capable of addressing these shifting threats?

Simonovich: We expect the threat environment will continue to escalate and evolve. To stay ahead of threats, companies should consider cyber security a core part of their business, and part of their design

requirements. In the energy sector, the life cycle of physical equipment is decades; many legacy sites were never designed with this threat environment in mind and thus are difficult to retrofit. Right now, the energy sector is starting to see the cyber security benefits of better automation, big data, artificial intelligence (AI) and machine learning. AI can use collected data to detect and prioritise threats, either intervening directly or highlighting anomalies. Machine learning can make updating detection capabilities easier. Automation can map system infrastructure and take a greater share of routine tasks. All these new capabilities share a common theme of making human analysts more efficient, with faster, better insights. Ideally, analysts will be able to devote a large portion of their time to investigating anomalies, detecting attacks at the earliest possible moment, and closing vulnerabilities before damage occurs. R&C

PERSPECTIVES

CYBER SECURITY REGULATORY RISK MANAGEMENT

BY **RICK BORDEN AND SAPHYA COUNCIL**
> FRANKFURT KURNIT KLEIN & SELZ

In the US, many companies' cyber security and IT operations are regulated at both the state and federal levels. The regulation has been inconsistent and confusing and is rapidly changing. For example, the Securities and Exchange Commission (SEC) requires public companies to disclose material information concerning cyber security, including filing a Form 8-K to report on significant events to shareholders. In 2022, the SEC proposed new public company rules that would require detailed disclosure regarding a company's policies and procedures to identify and manage cyber security risks, the role of management and the board in such policies and procedures, as well as a requirement for public disclosure of the details of material cyber security events within four days. The SEC also proposed detailed cyber security risk management and disclosure rules for investment advisers and investment companies.

The Federal Trade Commission (FTC) has enforcement power under section 5 of the FTC Act to bring an action against a company that commits an unfair or deceptive trade practice, which the FTC has enforced against companies that suffered from cyber security incidents. The FTC also oversees certain financial institutions under the Gramm-Leach-Bliley Act (GLBA), including the details of the Standards for Safeguarding Customer Information

under the GLBA (Safeguards Rule), which addresses cyber security.

At the state level, there are numerous cyber security requirements, some of which apply to all companies that collect, store or process personally identifiable information (PII) within a state, and some of which are sector specific. For years, Massachusetts had the most comprehensive cyber security regulation. Under the 201 CMR 17.00, every person that owns or licences PII of a Massachusetts resident is required to implement "minimum security standards" that contain administrative, technical and physical safeguards, including ongoing employee training, developing security policies, designating a person or persons to maintain the programme, and disciplinary measures. In 2019, New York enacted the Stop Hacks and Improve Electronic Data Security (SHIELD) Act. Like the Massachusetts cyber security regulation, the SHIELD Act also requires companies to adopt safeguards and implement a comprehensive security programme.

In 2016, the New York Department of Financial Services (NYDFS) promulgated 23 NYCRR 500 (Cybersecurity Regulation), which includes detailed cyber security risk management and technical requirements that go beyond protection of PII, for covered entities. The Cybersecurity Regulation was largely copied in a model law by the National Association of Insurance Commissioners. The Depository Trust and Clearing Corporation also recognised the Cybersecurity Regulation in its rules. The FTC amended the Safeguards Rule to incorporate many of the requirements of the Cybersecurity Regulation.

"The phenomenon of regulators using NYDFS-like requirements in their enforcement actions only stresses the importance of maintaining a comprehensive security programme."

Starting in 2020, the NYDFS began issuing consent orders and fining companies millions of dollars for cyber security risk management and technical failures. In light of numerous continuing cyber security breaches, the NYDFS has become increasingly aggressive in its enforcement of the Cybersecurity Regulation. In October 2022, the NYDFS issued a consent order with a $4.5m fine against EyeMed Vision Care LLC, a licensed health insurance company, for multiple violations of the Cybersecurity Regulation after the EyeMed email

mailbox fell victim to a phishing attack. Additionally, the New York attorney general fined EyeMed $600,000 under the SHIELD Act and the state's unfair trade practices act for the same breach.

Also in October 2022, the FTC appears to have used requirements substantially like the Safeguards Rule to regulate Drizly, an online alcohol ordering and delivery platform, even though Drizly does not appear to be subject to the GLBA. The FTC issued a proposed order against Drizly and its chief executive, James Cory Rellas, for conducting unfair information security practices and making deceptive security statements that compromised the information of more than 2.5 million consumers in violation of section 5 of the FTC Act. The FTC alleged that Drizly and Rellas misrepresented that the company used appropriate safeguards to protect consumers' personal information and failed to appropriately monitor its security processes, limit access to consumer information, require complex passwords, and implement multifactor authentication, which are requirements under the Safeguards Rule.

The phenomenon of regulators using NYDFS-like requirements in their enforcement actions

only stresses the importance of maintaining a comprehensive security programme, as well as assessing regulatory compliance on a regular basis. For companies to develop cyber security regulatory compliance programmes, they need to understand how cyber security organisations design substantive protections, as well as how the cyber security programmes map to regulatory requirements. The question companies need to ask is how they create a cost-effective compliance programme and reduce regulatory risk.

At the core of cyber security programmes are concepts that are based on financial controls. In general, information security programmes utilise controls from standards, such as the International Information Security Standard (ISO) 27000, the National Institute of Standards and Technology (NIST) 800-53 or Control Objectives for Information and Related Technologies (COBIT), in the development of the programme. Public companies use governance, risk and compliance (GRC) programmes to consolidate financial controls and document the testing of their effectiveness, so that the chief executive and chief financial officer are able to sign financial statements. Cyber security regulators are beginning to expect substantially similar activities. For example, the NYDFS regulation requires that the risk assessment policies and procedures document the manner in which the cyber security programme controls are tested for effectiveness.

For companies that have a well-established cyber security programme, developing a cyber security regulatory compliance programme requires a few additional steps. Cyber security controls must be mapped to cyber security regulatory requirements. There are GRC programmes that are used in cyber security, and many map to cyber security regulations. A cyber security regulatory risk assessment should be conducted – this is different from the standard cyber security assessment. The effectiveness of the cyber security regulatory controls should be documented. Risk mitigation and acceptance decisions should also be documented. All of this should be audited (or auditable).

Most regulations require cyber security risk assessments, but do not provide guidance on what is acceptable. This causes significant confusion for companies and exposes them to increased regulatory risk. The recent NYDFS proposal to revise the Cybersecurity Regulation includes more specificity in the content of the risk assessment, but even the new proposed language does not match to the requirements that were imposed on EyeMed in the NYDFS consent order. The FTC's Safeguards Rule does not detail the contents of the risk assessment. The SEC's proposed rules for investment advisers and investment companies requires that risk assessments be completed at a 'component' level.

Numerous companies currently have external auditors conduct System and Organization

Control (SOC)2 audits of their cyber security and IT programmes. While this is helpful, it may not be complete. SOC2 audits are not designed to map to cyber security regulatory requirements – rather, they are intended to identify cyber security risks. Risk assessments completed by cyber security consulting firms are also useful, but they are almost always aligned to a cyber security framework, standard or best practices regime. Internal controls testing is also very helpful, although only larger companies have internal audit teams that conduct these audits, and trained cyber security internal audit resources are hard to find.

To reduce regulatory risk, a best practices approach to cyber security regulatory compliance requires the development of a document that maps the regulatory requirements to the specific cyber security controls deployed by the company. Using the NIST Cybersecurity Framework as a pivot point is a useful approach. Using publicly available mappings of various regulatory requirements to NIST or ISO standards will help fill out a picture. Companies that take this approach will be viewed by regulators as being higher on a 'cyber security maturity model' scale, as it allows regulators to more easily see the manner in which the company ties their cyber security controls to the regulatory requirements, instead of the regulators being required to make their own interpretations. This does not prevent a regulator from disagreeing with the determination, but it reduces the chance of significant fines for non-compliance or ignoring regulatory requirements. A resulting cyber security regulatory risk assessment should then address all the regulatory requirements.

Third party and vendor management is also a major focus of regulators. For the most part, regulators do not have direct authority over vendors, so they place all of the management and oversight requirements on customers. This is very difficult for companies of all sizes. Large companies have a significant number of vendors and determining the real risk of each vendor is a complicated process. Smaller companies generally contract with larger, more established vendors that will not meaningfully negotiate contracts. Even the larger companies are unable to negotiate cyber security controls in contracts with the largest service providers. A critical approach to managing vendor risk in connection with cyber security compliance requires the structured identification, and risk rating, of vendors. The NIST 800-53 standard has tools that may be used to classify risks. Applying these tools to vendors, and classifying vendor risk with regard to confidentiality, integrity and availability of data and systems, allows companies to fine tune their risk acceptance and mitigation efforts. This approach is also highly useful to demonstrate to regulators why certain decisions were made with the highest risk vendors.

Most importantly, companies need to document cyber security regulatory risk decisions. These

decisions should be based on clear criteria and demonstrate the focus of the company on cyber security regulatory compliance. When a breach occurs, or another cyber security event occurs, and a regulator knocks on the door, it is too late to develop clear cyber security regulatory compliance documentation. Preparation is how cyber security regulatory risk is more readily understood and managed. R&C

Rick Borden
Partner
Frankfurt Kurnit Klein & Selz
T: +1 (212) 705 4884
E: rborden@fkks.com

Saphya Council
Associate
Frankfurt Kurnit Klein & Selz
T: +1 (212) 826 5575
E: scouncil@fkks.com

PERSPECTIVES

NAVIGATING THE RAPIDLY EVOLVING DATA PRIVACY REGULATORY LANDSCAPE

BY **DAFINA BUÇAJ**
> OCTILLO

The data security and privacy regulatory landscape is evolving dynamically. The wave of countries following the European Union's (EU's) approach to adopting comprehensive data protection legislation has increased rapidly in recent years. Brazil's Lei Geral de Proteção de Dados (LGDP), China's Personal Information Protection Law (PIPL) and South Africa's Protection of Personal Information Act (POPIA) are just some of the major laws adopted.

We are now seeing a wave of new and amended legislations in the US at state level, with the California Privacy Rights Act (CPRA), the Virginia Consumer Data Protection Act (VCDPA), the Colorado Privacy Act (CPA), the Connecticut Data Privacy Act (CTDPA) and the Utah Consumer Privacy Act (UCPA) all entering into force in 2023. Organisations are struggling to keep up with the requirements imposed by these laws. Multinational corporations are particularly faced with the challenge of navigating regulatory requirements across the jurisdictions where they operate globally.

Regulatory landscape

The majority of the laws adopted generally follow a similar approach and standards as the EU's General Data Protection Regulation (GDPR). Overall, these laws and regulations establish a general

framework for controlling and processing personal data, expanding the definition of personal data, outlining the responsibilities for privacy protection standards for data controllers and processors, granting individuals data subject rights with regard to their personal data, providing a private right of action, financial incentives, universal opt-outs, as well as outlining enforcement processes and penalties for violations of the laws. Overall, the laws provide stringent safeguards for personal data while demanding more accountability and transparency from the organisations collecting and processing personal data.

However, despite following similar trends, legislators are adding their own flavours and nuances by expanding on existing requirements and imposing stricter requirements for consent, international data transfers and protection of sensitive data. As a result, data controllers must comply with different standards and requirements with respect to the data they process depending on the jurisdiction where they operate. For global corporations, this implies addressing numerous laws and regulatory requirements, thus being exposed to higher risks of fines for non-compliance by data protection authorities. Hence, a robust data security and privacy programme will not only help minimise risk but also build resiliency and allow an organisation to adjust to new changes with more ease.

How to build a sustainable data privacy and cyber security programme

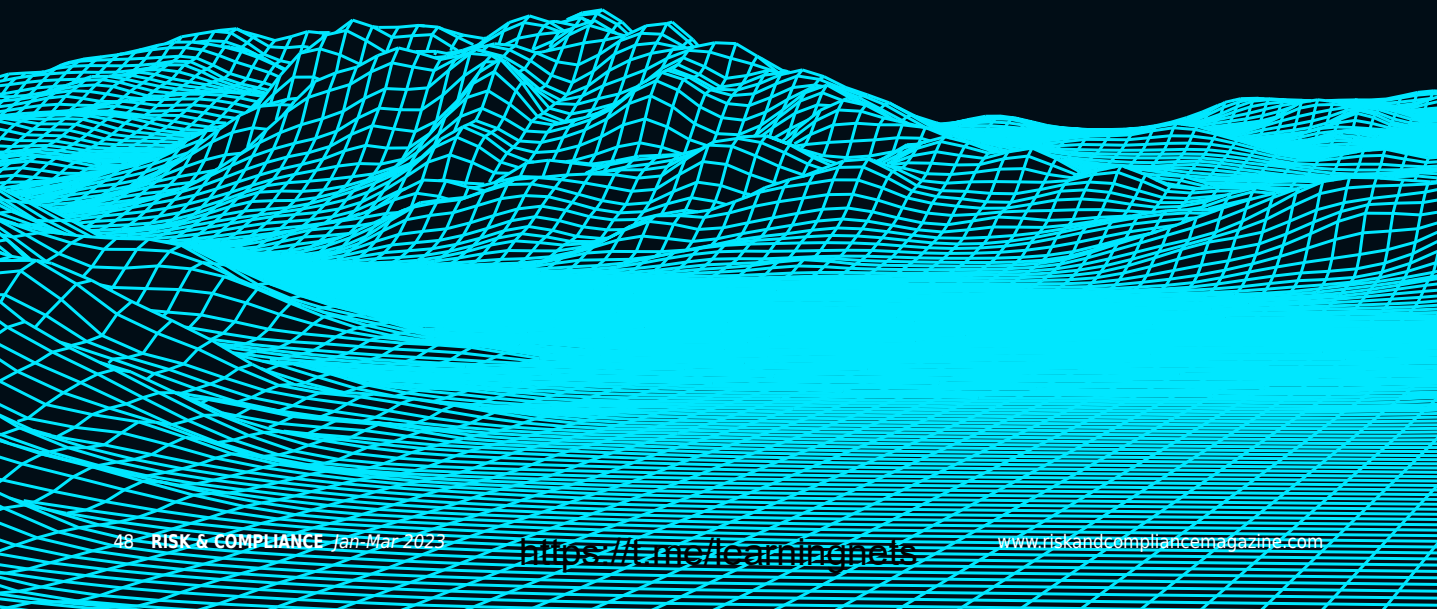
Building a sustainable data privacy and cyber security programme requires organisations to take a proactive and strategic approach. While each organisation will need to define what is the right approach for them depending on the nature of their services and operations, there are a few steps they can undertake to make navigating the fast-paced legislative changes easier: (i) identify what data they collect and process and where the data resides; (ii) conduct a regulatory assessment to evaluate the organisations' overall security and

"Data controllers must comply with different standards and requirements with respect to the data they process depending on the jurisdiction where they operate."

privacy posture, and determine applicable laws and regulations as well as compliance gaps within their existing programme; and (iii) prepare and implement an action plan to adopt the required privacy and security policies and implement them enterprise-wide.

Data mapping – know where your data is. Data is power but also a responsibility. The more data an organisation collects, the more likely it is to be exposed to regulatory, contractual and legal risks. The type of data collected and processed and the jurisdictions where it collects data can all impact the regulatory obligations to which an organisation may be subject. Most comprehensive data protection laws will apply to any organisation that collects and processes data of the residents of the country where the law applies. Some countries, like the US, predominantly follow the sectoral approach, so a particular law will apply to entities that collect and process data within a particular sector, such as the Health Insurance Portability and Accountability Act (HIPAA) for healthcare, the Family Educational Rights and Privacy Act (FERPA) for education and the Gramm-Leach-Bliley Act (GLBA) for financial services.

Very often organisations operate in a decentralised manner, making it challenging to gain a clear understanding of what data the organisation holds, for what purpose it was collected, how long it is retained and who has access to it. To better understand and answer all these questions, organisations will want to embark on an enterprise-wide exercise of identifying and mapping precisely what data they collect and the legal basis for collecting it, the nature and type of data, including where the data is stored and any third parties that



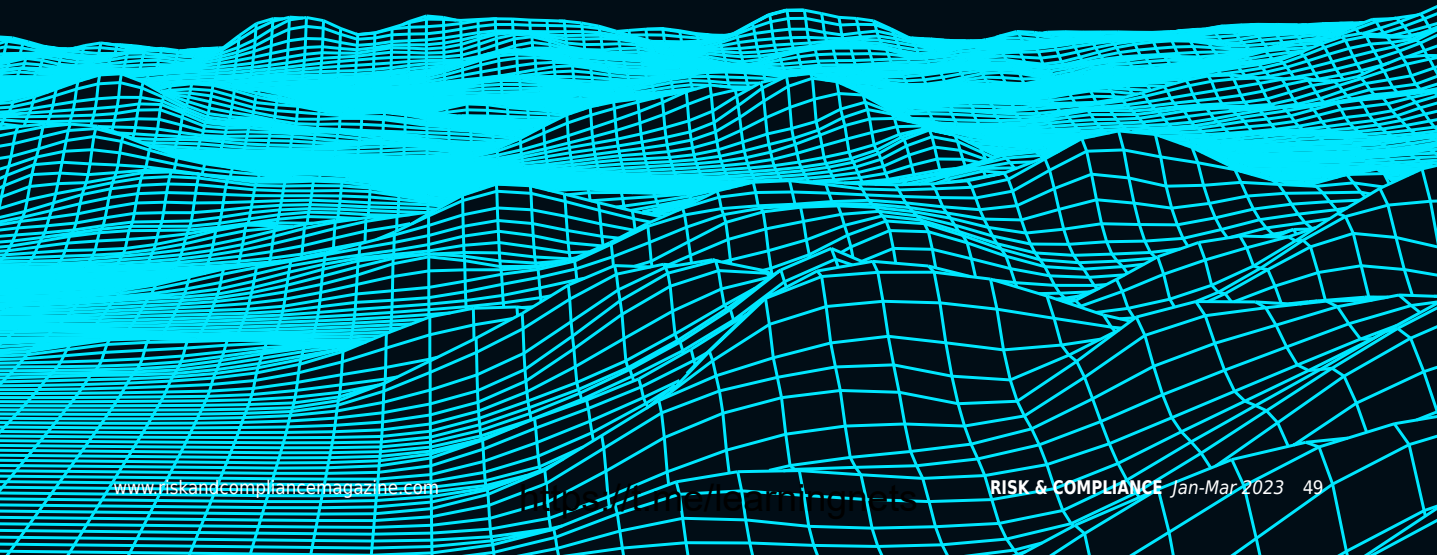
may hold or process data on their behalf and any international transfers of data.

Knowing what data the organisation collects and processes will not only help the organisation understand its regulatory requirements better, but will also help it comply with its obligations of data minimisation, retention, transparency, responding more effectively to potential security incidents and minimising risk exposures generally.

Regulatory assessment as a tool to identify gaps in compliance. For organisations of any size offering services and operating across jurisdictions, the main challenge is understanding what laws apply to their operations and what requirements are under these laws, and then determining a clear path to achieving regulatory compliance. To better understand their obligations under applicable laws, their current security and privacy posture and compliance with the legal requirements, as well as define a roadmap to build or improve their security and privacy programme, organisations can conduct a regulatory assessment.

Generally, a regulatory assessment is a tool which an organisation can leverage to evaluate its existing operations, identify any applicable laws based on the products and services it provides, its data collection and processing practices, the jurisdictions where it operates, and identify gaps in its existing security and privacy programme that require improvement to minimise risk and achieve regulatory compliance.

For example, if a corporation collects and processes personal information from customers in China and transfers this personal data to its affiliate companies in the US, the corporation needs to understand what the specific consent requirements are relating to collecting and transferring this data



outside of China (article 39 of the PIPL), including understanding the risks and consequences of failing to comply with these requirements. This may include evaluating the existing transfer tools the corporation relies on, as well as the technical and security safeguards it has in place to safeguard data.

Similarly, if the corporation operates and collects personal data across the US, it will likely need to evaluate whether it meets the threshold determined by the CCPA and the CPRA and new legislation in Colorado, Virginia, Connecticut and Utah. If its practices of collecting and processing personal data fall within the scope of these laws, the corporation will need to further determine what steps it should take to comply with the new requirements imposed by these laws.

In addition, an assessment can help organisations better understand their current security and privacy posture and identify gaps between their existing programme and the regulatory requirements. As such, the assessment can include specific recommendations on narrowing these gaps and coming one step closer to regulatory compliance.

Developing a data security and privacy programme. An organisation's security and privacy programme should reflect the requirements deriving from various laws and regulations. A programme will be sustainable if it is comprehensive and can easily adjust to new laws. Although challenging, walking through these steps helps to identify gaps in compliance and can help to define a clear roadmap to address some of the most significant regulatory requirements.

A clear approach and strategic direction that an organisation will take toward privacy and security are essential. Applicable laws provide different standards of protection for personal data. Organisations may find it easier to comply with the less stringent requirements. However, despite being more challenging to implement, choosing to comply with more stringent standards is advised. This approach can result in a more durable security and privacy programme that will be easier to adjust to newer laws with similar or less stringent requirements.

A data security and privacy programme should be built upon a good foundation and proper governance structures. Organisations should determine a clear governance structure and oversight at an executive level. Furthermore, organisations should seek to document their privacy and security policies and procedures, including determining roles and responsibilities, establishing appropriate standards and controls, and outlining procedures for implementing such controls.

A comprehensive approach to privacy and security compliance will address, at minimum, the following areas: information privacy, information security, HR data management, incident response management, third-party management, risk management and

international data transfers. Based on the data they process and the jurisdictions in which they operate, organisations should adopt policies that outline their overall approach to data protection and compliance with privacy principles, and determine the standards for collecting, processing, classifying and retaining data.

To comply with upcoming laws, organisations will need to review and revise their existing external-facing notices, internal polices for responding to data subject access requests and provide opt-out mechanisms. Similarly, organisations can adopt adequate policies for managing HR data, mitigating third-party risks and complying with international data transfer requirements.

Furthermore, to comply with information security standards and best practices, organisations should adopt information security policies that determine standards and controls to protect the confidentiality, integrity and availability of data, as well as concrete guidance and steps for handling incidents and mitigating risk. Lastly, organisations will need to allocate adequate resources to implementing the security privacy programme, review upcoming laws and continually improve their programme. R&C

Dafina Buçaj
Data Privacy Attorney
Octillo
T: +1 (702) 465 1582
E: dbucaj@octillolaw.com

PERSPECTIVES

INTEGRATING RISKS INTO STRATEGIC DECISION MAKING

BY **SUMIT CHATTOPADHYAY AND MINGYUAN ZHANG**
> SAS

Integrating risks into strategic decision making is both rewarding and challenging. With a robust, scalable architecture and integrated analytic platform, firms can overcome the challenges and achieve a dynamic integration of risk and finance for maximum return.

Strategic decision making under uncertainty

Firms make decisions continuously regardless of substantial uncertainty. Risk is the potential financial loss a firm can incur. Risk management is the art of mitigating potential losses while managing a going concern and maximising risk-adjusted returns. Historically and traditionally, enterprise risk management (ERM) was considered primarily for compliance management and protecting the value of the enterprise.

The global financial crisis uncovered the gap between the risks that financial institutions (FIs) took and what their boards of directors perceived to be taking. The gap implies that the top risks that impact strategic objectives are not properly accounted for. To address this gap, organisations should pivot to a more quantitative way of identifying and measuring key risk indicators (KRIs). Analysis

of KRIs and their relationship to other financial metrics can reduce business volatility and enhance financial performance. It also helps balance trade-offs between short- and long-term earnings of the company.

Therefore, ERM should create value by integrating with business performance metrics. To drive this value creation, it is critical for FIs to understand and analyse the ever-changing, dynamic relationship among strategic goals, value drivers, and risk factors such as credit, market or macroeconomic risks. With careful expansion and the leveraging of their ERM assets, a firm can make risk-informed business decisions by incorporating risk measures into strategic business and financial planning. When making financial decisions, a chief financial officer (CFO) may consider many financial factors including balance sheet, income statement, cashflows, profitability, customer lifetime profitability, and so on. At the same time, a CFO must also consider those factors in the context of risks, and examine their key drivers, such as macroeconomic conditions, idiosyncratic risks, customer credit ratings and defaults, and so on. Understanding the intricacies of risk versus opportunity enables a firm to maximise risk-adjusted returns.

Incorporating risks into financial decision making

What do we mean by 'incorporating risk in financial decision making'? This represents a seamless flow of data and information within an organisation to derive a better understanding of risk and the financial implications of decision making. Risk and finance can share common data, models, economic scenarios, analyses, workflows, and so on. This can not only lead to greater insights of business drivers, but can also significantly improve process efficiency, consistency and transparency and reduce redundancy and potential human errors.

> **"It is important to model not only the physical impact but also policy and social responses to it, as well as the longer term impact that may end up being more severe."**

The integration also needs to be 'dynamic'. Being dynamic means the integration process will be achieved and continually enhanced in a well-controlled and automated environment. One of the

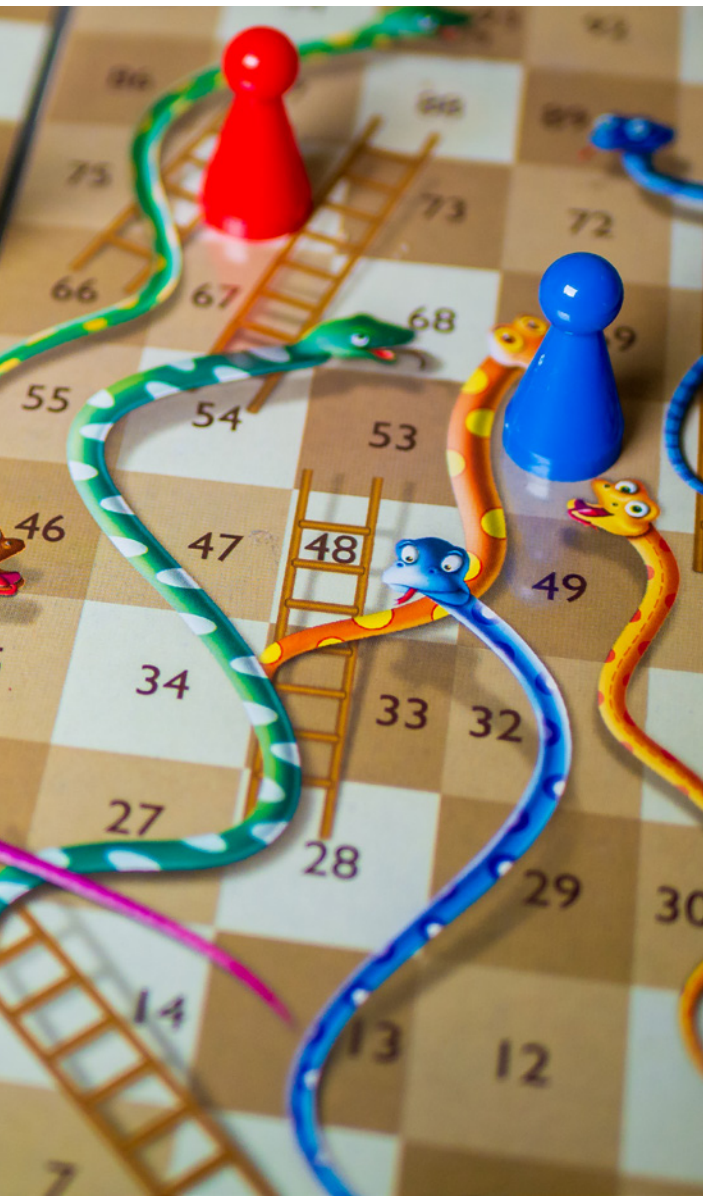
key use cases is to perform stress testing of financial statements under multiple risk scenarios across time horizons based on a set of assumptions regarding changes in portfolios and economic factors.

The vision of integrated balance sheet management stipulates using 'best of breed' models across the enterprise on an integrated analytic framework that affords a dynamic integration of risk and finance. This approach is relevant for both financial and non-financial firms, as it helps them overcome many issues like data reconciliation, relating data about risk and return, improving financial planning, key performance indicators (KPIs) and ultimately enterprise profitability.

Understanding the dynamics between risk and finance

One of the greatest values of having a robust scenario analysis framework in place is an improved ability to quickly incorporate new and changing information into projections. It can be used to truly understand and model the dynamic relationship between financial performance and risk drivers and how they align with organisational goals. Such an exercise is only feasible with a well-developed scenario analysis capability and true integration of risk and finance.

Scenario-based risk management offers the potential to go beyond regulatory compliance. It can be a holistic process that considers the impacts



on all aspects of the balance sheet with consistent assumptions and modelling techniques. The holistic perspective then enables the next step: optimising the use of capital and liquidity. It provides senior management with critically important information on the possible outcomes of their actions, such as business growth and origination strategy, capital usage, dividend policy, contingency planning and so on. It helps them answer business planning questions, such as how are they going to grow the balance sheet? What is the origination strategy to get an optimal asset mix? How are those assets going to be funded? What happens to those plans if the environment changes? How will the dividend policy be impacted? These are important questions that banks face on a regular basis.

Furthermore, scenario analysis allows FIs to model and quantify the impact of multiple variables with non-linear relationships on target-dependent variables. The variables in the business and socioeconomic world – such as the current crises in Ukraine, demand and supply dislocations, and the impact of climate risk do not follow well-governed rules. In those cases, it is important to model not only the physical impact but also policy and social responses to it, as well as the longer term impact that may end up being more severe.

Ultimately, the most important by-product of this exercise is establishing an integrated balance sheet and risk management framework. This is

the pinnacle of risk and finance integration. On the one hand, scenario-based risk management transformation can help improve risk-adjusted returns via better informed and timely decisions. On the other hand, without dynamic integration of risks and finance, it is impossible to fully unlock the benefits of scenario-based risk management.

Challenges and key considerations

Traditionally, finance focused on merely reporting what happened in the previous periods. Quantifying risk was not given sufficient focus. When crises unfolded, the lack of an integrated and comprehensive risk and finance system became a huge problem. And even though many FIs have spent a lot of effort on this, it remains incomplete at best. Several reasons explain how and why it is difficult to incorporate risks into financial and strategic planning, as outlined below.

Organisational alignment. Effective collaboration and communication across different business units is critical. Organisational structure, the processes and controls, and human talents must be supported at the highest levels. Without organisational alignment and buy-in at the highest level, this integration cannot be achieved. However, for many organisations, conventional ERM programmes remain largely disjointed from strategic planning. This disconnect means that ERM is not well positioned to add organisational value by informing business decision making and ensuring that limited resources are allocated to the most significant risks.

Data management. Data management is foundational for risk and finance integration, but it is also the most expensive and time-consuming part of the exercise. Being able to capture, integrate, analyse and draw insights from those diverse data sources remains a huge challenge for many FIs. There are several reasons for this challenge. First, most organisations still have data silos, where data resides in multiple sources or databases – relational or non-relational databases, sometimes in files, in data lakes, or in the cloud. Data also comes in a variety of shapes – it can be time series or cross-sectional, it can be text, visual or audio. Second, data quality checking and correction remain a manual, labour-intensive process, resulting in higher costs and compromised analytic results. Many FIs still do not have the underlying technology that can help them effectively track, validate and improve their data quality in a consistent and automated process. Third, there may be a lack of established data governance within the organisation. Almost every financial regulation emphasises the importance of data governance – indicating which data should be captured, how far back in time you should go, how to aggregate and disaggregate the data, which assumptions can be used, and so on. FIs are expected to trace the data from general ledger entries to the data sources, even if data has been

transformed multiple times during this journey. However, many FIs do not have a data model that is flexible enough to support onboarding of new data while maintaining data lineage and auditability in an open framework.

Model operationalisation management (ModelOps). In order to deploy models into production, FIs must ensure all models are stored in a single model inventory as part of model management and are evaluated properly against other contender models. Models should be documented properly and fully tested and validated, and model performance must be monitored and enhanced over time. However, for many FIs, models are often located in a business unit silo with a lot of duplication across the organisation. There is not a centralised model inventory on a common platform for them to evaluate, manage, monitor, track and execute models in a seamless mode. Therefore, ModelOps often turns out to be an extremely time-consuming and expensive process. FIs often need to deal with two critical modelling issues: model limitations and model transparency. Any model is an imperfect representation of reality because reality is infinitely complex and cannot be perfectly reduced to a mathematical formula. This is especially true for the financial services industry, as new rules and policies are constantly introduced, forcing market participants to respond accordingly. Therefore, assumptions must be made to simplify reality, and these same assumptions also cause model imprecision. To overcome model limitations, a firm needs the ability to run, compare and validate models against portfolios, profit and loss, business growth plans and financial statements under multiple scenarios in a cohesive way. This also helps achieve greater model transparency, which is of paramount importance. A thorough understanding of model risk and limitations is essential if an FI is to use them responsibly. A firm must develop a clear understanding of model assumptions and conditions associated with each scenario on a probabilistic open framework.

Having an integrated analytic platform is the key to dynamic integration of risk and finance

Management decisions that impact balance sheet growth, loss mitigation, capital issuance and return are influenced by factors across the risk spectrum. It is critically important to consider all of them from a connected system perspective. To make this integration work, FIs must combine data management, models, scenarios, analytics, business intelligence, governance and application architecture. All of these should be components of a technological platform that allows data from multiple sources to be accessed, modelled, analysed, reported and audited. This inevitably leads to an integrated analytic platform that is built on technology to leverage the value of consistent and

common data, models, analyses and tech tools. This platform should not only provide a retrospective, reporting-focused 'business as usual' view, but also offer the ability to incorporate various risk and business scenarios into the financial planning process. With that, companies can measure the impact of exogenous shocks, like the coronavirus (COVID-19) pandemic, global temperatures rising by 2 degrees Celsius and others, on financial indicators like revenue, net profit margin, net cashflow or capital ratios, all on the same platform. Such a platform would likely require companies to leverage a number of technology advancements.

Digitalisation of risk and finance. The digitalisation of risk and finance is an absolute necessity for this dynamic integration. Digitalisation helps provide consistency, efficiency and organisational discipline in decision making. It is important for the FI to make different decisions based on the same fundamental set of data, assumptions and analytics. Having an integrated analytic platform can help an FI see the big picture and make better informed decisions that can translate into superior competitive position.

Robust and scalable architecture. A single unified data, analytics and visualisation platform is built upon robust and scalable architecture. With that, an FI can integrate a multitude of different data sources, including structured, unstructured and real-time data, and, if needed, obtain real-time analytics on data or market states. The system should have high throughput for processing big data and analytics, world-class predictive modelling, and machine learning techniques with different programming languages and development environments. It should also offer visualisation capabilities, and low-code and no-code applications to different individuals within the organisation.

Risk platform modernisation. Risk and finance integration is methodologically challenging, time consuming and costly. To address that, infrastructure must be modernised to remove extensive manual work and system constraints. As a result, the integrated analytic platform can provide a coherent framework that allows for holistic forecasting on a much broader spectrum. This includes all key asset and liability segments, capital, credit impairments, dividend, income and taxes. Furthermore, this platform should be transparent, providing a fully auditable log to regulators and auditors. This will ultimately lead to better risk-informed decisions.

Conclusion

The benefits of integrating risks into finance for strategic decision making is obvious, but there are significant challenges posed by the infinite complexity of reality. With a trusted technology partner in analytics and risk management solutions, and by rationalising the data, scenarios and models on an integrated analytic platform, an FI can achieve

a true dynamic integration of risk and finance to gain invaluable business insights. R&C

Sumit Chattopadhyay
North America Head, Risk & Finance Advisory
SAS

Mingyuan Zhang
Principal Solutions Architect
SAS

PERSPECTIVES

THE BILLION-DOLLAR RISE OF NON-FUNGIBLE TOKENS

BY **ANDREW KAKABADSE AND NADA KAKABADSE**
> HENLEY BUSINESS SCHOOL

Digital technology developments such as blockchain provide a network-based technology solution that is used to record transactions efficiently and securely, and the most popular cryptocurrency – Bitcoin – has stimulated a mass of new retail and institutional investor growth.

This heightened speculation of opportunistic investments has revolutionised the financial ecosystem and resulted in the introduction of non-fungible tokens (NFTs), a blockchain product that has gained significant public attention in recent years.

NFTs exist as unique digital token assets which represent tradable digital goods, such as collectable art, profile pictures, sports cards, videos, music and in-game items.

Although sceptics have mocked NFTs as being simple digital images that can be just as easily copied and pasted, the NFT has become one of the most utilised components of the Ethereum ecosystem, creating a billion-dollar economy.

The unique value of NFTs

An NFT is a unit of data stored on a blockchain. It certifies a digital asset is unique and, therefore, non-interchangeable, while offering a unique digital certificate of ownership. As a result, an NFT can be equated to being a proof of ownership.

The unique value of NFTs signifies them as being 'non-fungible'. In other words, they cannot be traded, but the digital asset they represent can be. The NFT's function is to guarantee the value intended by the creator, for an owner or buyer.

The NFT market began to attract attention in February 2021 when 'CrypoKitties', an NFT digital collection of artistic images representing virtual cats used in a game of Ethereum, allowed players to purchase, collect, breed and sell 'cats'. The emerging purchases made in-game using cryptocurrency reached £1.5m in value.

In March 2021, the Nyan Cat, designed by the artist Beeple, was auctioned and sold for the equivalent of $650,000 as an NFT at Christie's, making it the third-highest auction price achieved by a living digital artist.

Similarly, the Board App Yacht Club, a vastly popular NFT collection of gaudy primate cartoons, has become an NFT status symbol for millionaires and pop stars by trading at more than $1m apiece.

As the crypto art market has boomed, NFTs have started to be taken more seriously. Many digital artists operating outside the mainstream contemporary art sector rushed to embrace NFTs as a means of selling their work. New crypto artwork communities sprang up to feed the market, building

on NFT platforms such as OpenSea, Hic et Nunc and others – all of which gained prominence overnight.

NFT market growth is extending into publicly traded partnerships, creating competitive individualism and promoting the cult status of genuine artists. For most artists, it is attractive to earn a living that funds their work by cooperating with the market. However, there is a downside, as with all markets: the emergence of NFTs also produced inequalities, monopolies and fragility.

The value add of community

So why would an investor be enticed by NFTs? A key motivation, fully reinforced by the wider industry, is a notion of 'community'. Investors stress that establishing a community within an NFT project is a precondition of success, as though this automatically ensures inbuilt value.

In the words of one investor, "NFTs are all about the community, because this is how popularity and virality are created, leading to a shared belief of investment value".

Social media is seen as the epicentre of community. This influences changes in the valuation of NFTs, with another investor adding "social media is there as a bridge between buyer and seller, and these bridges only increase with stronger communities and so reflect higher demand for the NFT".

The greater the number of members a community holds, the greater fluctuations in demand become, along with asset scarcity. All of this makes investment look distinctly attractive.

In reality, social media influences and controls pricing. The scale and size of a community determines price shifts on the secondary market. The level of attention this receives is a direct result of social media's impact.

One NFT owner comments: "The secondary market is where prices can significantly fluctuate, usually in a positive manner if retention is high, which is typical in a strong community." The reason behind this is that more meaningful interactions between buyers and investors are taking place. The more popular a certain NFT is, the more valuable it becomes.

Furthermore, social media impact is directly linked to potential profit margins. Achieving a higher floor price with social media emphasises a shared belief in an online community. This strengthens reputation and enhances higher monetary value margins.

Another NFT investor comments: "As far as a blue chip, the same case is for the NFT still having value, but with a smaller community the price concerns over purchasing are much lower, and there is greater concern of collapse due to a lower level of reinforcement in belief."

Although social media can seriously influence price controls, the important point to note is that the decentralised NFT market is unpredictable.

"The whole crypto industry is too volatile right now," notes one buyer.

Social media has the capacity to establish a distinct brand image and a certain level of stability for an NFT, but the strength of the community is the ultimate determining factor.

A key motivation of social media is to create money opportunities for both creators and investors. And yet, the decentralised and distributed state of the online market still has buyers and sellers shaping the desirability of the digital object.

and sellers are made up of only a small niche of collectors.

"Despite growing importance, the digital economy is still in its early stages – particularly when it comes to challenging the value of physical objects."

The price paid for NFTs

How valuable is an NFT? If buyers and sellers are determining digital object desirability in a decentralised and distributed online market, who can say exactly? Dramatic fluctuations occur as NFT markets are highly illiquid in nature, with sale prices proving to be volatile and irregular.

Price prediction models have been used for raw data value sets for cryptocurrencies, but the currency adopted to determine NFT-worth remains in US dollars. To date, a price prediction model is not available for NFTs. The recent emergence of this market and relatively low number of transactions per NFT make accurate valuation highly challenging. Despite community size advantages, NFT buyers

Despite this, NFT value is clearly determined by four factors: (i) authentication; (ii) collection; (iii) ownership by collectors; and (iv) NFT sale history and visual features. The combination of these factors is usually a reasonable indicator of price.

One NFT buyer explains: "Typically, an NFT has value because buyers and the rest of the community believe it does. That is true for all art and collectables. Also, the social proof associated with the project behind an NFT may be a decisive factor in determining its value."

Authentication leads to digital asset verification. Determining the owner of a work of digital art ensures ownership and originality. Overall, authentication is hard to create due to the unlimited

access to digital art, but being awarded NFT status validates authenticity.

In comparison to traditional physical art, NFT value requires a limited-edition supply of work, which gives the artist credit without impersonation. While access to digital art is open (i.e., creators and artists post-NFTs under their social media platforms), authenticity can remain questionable should impersonation occur. As such, value is often profoundly impacted.

NFTs registered on the blockchain secure the assets against vague authenticity, acting almost as a certificate. Validating the creator's presence online on social media without the risk of being discredited, is essential.

Reputation, brand and social media

While NFTs are traded on blockchain using cryptocurrency according to the value of exchange assigned to them, the value of the art is often subjective and determined by the creator's persona or the narrative associated with that image.

One NFT creator explained: "Social media is there as a bridge between buyer and seller, and these bridges only increase with stronger communities and reflect higher demand for the NFT."

An NFT as a piece art could have cultural significance through its perceived attractiveness, history of ownership, or other personal attachments that determine its valuation. Similarly, the key driver of an NFT's value depends on the artist's reputation and brand.

Despite growing importance, the digital economy is still in its early stages – particularly when it comes to challenging the value of physical objects. The key question remains: what is the digital impact of any contribution? Assets such as websites, domains, social media profiles, friends and professional networks – all have a tangible impact on NFT valuation.

Another NFT investor adds: "Everything encompassed by Twitter can influence NFT valuations. Follower count is the most important because it is a primary reflection of community strength, but something as small as collective posts on a topic, or retweets from an influencer or industry expert speaking about a project could also positively or negatively influence an NFT's value."

Reality bites

For investors, the most important feature of an NFT is social popularity.

The value of the project is determined by the quality of utilisation for building community and brand image enhancement. The ultimate price achieved at sale is the outcome, shaped by social media's focus on a community's growth and value.

This is comparable to the traditional art world. Vincent van Gogh, today world renowned, was

generally despised in his lifetime. Many of his outstanding art works were used as target practice.

While he was alive, van Gogh's family hid many of his most treasured artworks so they would not fall into the hands of the ignorant and destructive. After his death, his family campaigned for him to be recognised for his worth and achievements as an artist, building a community that today values van Gogh's paintings in the multimillions.

Similarly, Salvador Dali's fame came largely through the recognition of his work by the New York artistic community. There was little support from his country of birth, Spain, and so little or no value was attached to his paintings.

For many, NFT purchase is driven by the emotionally satisfying experience of community – but looking to the future, an unwelcome challenge is rising.

Owing to the growing volume of transactions, networks can become overwhelmed, resulting in a sharp rise in congestion fees. As a result, by attempting to secure a rare NFT, the bidder is now often paying a premium to ensure their transaction is expedited.

High transaction fees are undermining the very principles of community. Instead, they create a financial derivative, or materialise as a type of gaming which prices certain community members out of transactions.

For buyers and sellers, community is becoming an end in itself. For investors, community is simply the means of determining value, a principle that has been the foundation of the traditional art world for hundreds of years. While the technology is new, the same old principles apply. R&C

Andrew Kakabadse
Professor of Governance & Leadership
Henley Business School
T: +44 (0)1491 418 770
E: a.kakabadse@henley.ac.uk

Nada Kakabadse
Professor of Policy, Governance and Ethics
Henley Business School
T: +44 (0)1491 418 786
E: n.kakabadse@henley.ac.uk

PERSPECTIVES

THE IMPORTANCE OF A STRONG RELATIONSHIP BETWEEN COMPLIANCE AND BUSINESS TEAMS

BY **SARAH FOLEY AND FELIPE MONTOYA**
> PATTERSON COMPANIES, INC.

The partnership between an organisation's compliance team members and internal business stakeholders is critical in building a culture of compliance, enabling the business and protecting a company's corporate reputation and operations from potential regulatory and legal risks and scrutiny. A proactive relationship between compliance team members and internal stakeholders cements critical and sustainable compliance processes throughout an organisation. Further, many regulatory agencies have memorialised expectations that underscore the need for commitment from business partners as it relates to an organisation's compliance programme. Companies should consider various aspects when solidifying this relationship, as outlined below.

Encourage a commitment to compliance. A commitment to compliance cannot be forced, but it can, and should, be emphasised throughout an organisation. Compliance is essential for any organisation. It strives to ensure that a company and its employees follow regulatory and legal requirements, and internal policies and procedures, upholds an organisation's values and culture, and meets its duties to stakeholders. Business partners that are committed to compliance understand and recognise that their actions, regardless of how large or small, impact an organisation's

compliance programme and overall corporate culture. Business stakeholder accountability for compliance is also an important component to bolstering a company's commitment to compliance. An organisation's compliance team can help drive internal partners' accountability by sharing the compliance programme's priorities, engaging in ways to assess whether compliance goals support and align with commercial initiatives, and through transparent dialogue that encourages a 'speak up' environment should a potential concern be identified, or specific risk require remediation. Additionally, internal partners play a crucial role in the implementation phase of compliance initiatives, which reinforces the need for that strong partnership. It is imperative for compliance teams to effectively communicate the purpose of a corporate compliance programme, which helps internal partners act intentionally and view themselves as having an impactful role in compliance.

Help employees understand the 'why'. The 'why' of compliance drives an organisation's efforts. In his book, 'State with Why', Simon Sinek states, in part, that an inspired company (and leaders) "thinks, acts and communicates from the inside out", which helps articulate 'why' companies do what they do. When business stakeholders understand from their compliance partners the 'why' behind specific compliance initiatives or proprieties, as well as the consequences of non-compliance, they appreciate that a compliance programme helps protect the 'health' of the organisation, as well as meet legal and regulatory obligations. Understanding the 'why' also helps business stakeholders feel that they are part of the solution, which enhances the connection they feel to the company. Additionally, compliance becomes even more critical when commercial and operational issues are more complex as businesses grow. Perhaps the obvious 'why' of compliance is to reduce risk, build trust among a company and its consumers and stakeholders, facilitate the right actions by employees, and surface misconduct. However, compliance also inspires leadership and innovation to define what an organisation does and

"Many regulatory agencies have memorialised expectations that underscore the need for commitment from business partners as it relates to an organisation's compliance programme."

why it does it through aligned values that help drive value and growth.

Compliance supports strong commercial performance. A strong partnership between compliance and business teams helps boost employee productivity and efficiency, reduces and mitigates risk to the business, and provides insights that help an organisation make smart business decisions. Compliance is needed to compete commercially by enabling the business to meet specific industry or regulatory requirements. Being able to articulate to consumers that your organisation takes compliance seriously can provide a competitive advantage and help it avoid any entanglement in a regulatory inquiry or investigation. It also can save an organisation money by avoiding significant fines and other penalties for non-compliance. After all, what would be the point of making revenue now, when it would be lost later because things have not been done the right way? A robust compliance programme can help provide clarity around specific processes that support commercial initiatives and, in turn, provide business value, which can help drive revenue upward. When implemented appropriately and followed, a compliance programme can protect a company's brand and reputation, increase confidence in consumers in an organisation's products or services, mitigate disruptions that could derail strategic priorities, and be a partner in growth opportunities.

Compliance teams need to understand commercial strategy. The compliance landscape is constantly evolving, and if a compliance team does not understand its organisation's strategic imperatives or commercial drivers, the advice it provides is not relevant or effective in addressing risk, potentially limiting the success of the company's objectives. Compliance teams can, and should, be key strategic business partners. Often, a compliance programme is viewed as 'red tape' that slows down an organisation's go-to-market or growth strategies. However, when a

compliance team has visibility into business goals, and a 'seat at the table' when discussing them, it can advise on compliance matters in a way that proactively identifies and mitigates risk, protects the company's brand and reputation, and bolsters an organisation's competitive footprint in the marketplace. This reinforces the case that a robust compliance programme is a key function to help drive revenue upward.

Mitigate risk through collaboration with business partners. While the 'why' is important when establishing and maintaining an effective compliance programme, equally important is the 'how', which is accomplished primarily through a sound collaborative relationship between compliance teams and business partners. In almost all situations, collaboration between business partners and compliance teams results in better commercial outcomes because it allows a consistent model for an organisation's operations that meet specific compliance requirements. An effective and collaborative framework with a compliance team enables speed to market for commercial teams because of increased transparency as it relates to decision making. Compliance is everyone's responsibility at a company, and compliance and commercial teams have the same goal: to drive growth and protect revenue. While a compliance team establishes compliance-related controls, policies, procedures and training for all company employees, ownership needs to be embraced by all at an organisation. Building bridges between compliance and business teams helps the sharing of information and coordination on risk remediation. Critical to the success of this is a compliance team approaching issues with a business perspective and making recommendations to address compliance issues with an appreciation for and interest in the business. A close partnership with the business helps ensure that compliance requirements are not obstacles to operations, are tailored to address specific risks to the business, and provide benefit to

an organisation. This also builds a proactive culture that helps address risks in a much quicker manner, potentially resulting in lower costs, versus a reactive culture that acts after the risks have become much larger and more expensive.

Compliance teams should not be inflexible nor barriers to an organisation's business operations and strategic priorities. Rather, compliance should be a partner to help ensure success. Business stakeholders providing a seat at the table for the compliance team helps guarantee that compliance requirements are integrated into strategic plans and offers visibility to commercial goals or new business strategies, resulting in efficient support and risk identification when an organisation wants to launch a new product or service, enter a new market category or expand its operational footprint. R&C

Sarah Foley
Deputy Compliance Officer and Director of Compliance
Patterson Companies, Inc.
T: +1 (651) 405 5116
E: sarah.foley@pattersoncompanies.com

Felipe Montoya
Compliance Manager
Patterson Companies, Inc.
T: +1 (612) 619 2821
E: felipe.montoya@pattersoncompanies.com

PERSPECTIVES

A 'PRE AND POST' APPROACH TO COMPLIANCE

BY **JAY M. COHEN**
> GIORDANO, HALLERAN & CIESLA

What is the proper role of the compliance function in an organisation? How can the compliance team best contribute to the growth and success of the firm? Despite the decades-long development of compliance into a valuable and valued function, compliance officers and their companies still struggle to answer these questions.

From time to time, a great debate erupts in the compliance community – generally fuelled by a new set of rules and regulatory expectations to meet – about the responsibilities of the compliance function and team. As one example, many companies are still trying to figure out whether compliance or information security, or some other unit, should 'own' data privacy and security.

This debate has been re-energised lately, driven by the focus on environmental, social and governance (ESG) issues, and the explosion of laws and regulations that has come with that attention. Companies of every size and industry face enormous challenges from the constantly-evolving and ever-expanding regulatory requirements and risks regarding ESG. In this environment, with its confluence of rising expectations for compliance and shrinking tolerance for failings, compliance officers have their own challenges to both help their companies find the right overall responses, and to

identify where they best fit in to ensure that those responses have been implemented and are working.

Not surprisingly, compliance officers are reacting in wildly-divergent ways, ranging from "compliance should lead ESG" to "ESG is not our job". A survey reported by Compliance Week in November 2021 reflected this diversity, finding that: (i) 13 percent of compliance officers said they had primary oversight for ESG in their organisations; (ii) 24 percent played the role of adviser; (iii) 27 percent were members of an ESG committee; (iv) 9 percent said they were an "advocate"; and (v) 25 percent had no role in ESG at all.

That said, a different approach is required, one that compliance officers should follow for ESG and every other set of laws and regulations that their companies face, regardless of whether the compliance officer is also an adviser on data privacy and security, or the member of an ESG committee, or none of these.

Whatever the issues, the following four questions should be answered. First, what are the regulatory requirements and risks for the company – based on its size, industry, products, markets, geography, distribution, organisation and other relevant factors? Second, what does it take to comply with these rules and mitigate those risks? Third, has the company operationalised the needed controls for compliance? Finally, are those controls working and how does the company know?

"Companies of every size and industry face enormous challenges from the constantly-evolving and ever-expanding regulatory requirements and risks regarding ESG."

While the answers will vary from company to company, the questions should be the same.

This is the 'pre and post' approach to compliance – with the first two questions representing the pre (what is compliance for us?) and the third and fourth the post (are we complying?). Not only will this work for any company, it also meets the expectations of courts and regulators and follows the blueprint of compliance experts.

In refusing to dismiss a lawsuit accusing the directors of a food producer of failing to do their jobs, the Delaware Supreme Court noted that the board presided over a company where "no reasonable compliance system and protocols were

established" to address "the most central consumer safety and legal issues facing the company". Likewise, the US Justice Department, in deciding if a company has an effective compliance programme, asks, "whether the company has analyzed and addressed the varying risks presented by the location of its operation, the industry sector, the regulatory landscape, potential clients and business partners".

In its answer to what compliance should do about ESG, the Ethics and Compliance Initiative (ECI) explained that compliance should "exercise its role as a controls function, overseeing compliance risk management, setting policies, overseeing compliance training and communications, managing the [helpline] program, conducting investigations and fostering a culture of compliance". In short, compliance should help firms understand and address the applicable rules, and figure out if they are meeting these obligations.

So, how does this pre and post approach work in practice, and what does it mean for compliance professionals? In this framework, compliance is responsible for the pre and the post, with the rest of the company responsible for all the work in-between.

The pre approach. What are the rules and regulations that apply to the organisation, and what will it take to comply with them? What are

the 'mission critical' rules within this universe – the ones the company must get right? And how does the company know what these rules are? How does the company keep up with changes in laws and regulations – assessing them, educating impacted business partners and then overseeing compliance with them?

The post approach. Is the company complying with these laws and regulations and how does it know? What data and other indicators – whether generated by compliance, internal audit, customers, regulators, the business, or any other sources – tells this story? How is this information collected, organised, recorded and reported? And what mix of data, tools, technologies and expertise – within compliance and throughout the organisation – will create the most value in addressing these laws and regulations?

The hard and necessary work in-between to be compliant can, and usually will, be done elsewhere in the company – whether it be in product development, sales, marketing, finance, information technology, human resources or mergers and acquisitions – but compliance must make sure that the pre and the post are covered.

A successful pre and post approach to compliance can be aided by the effective use of: (i) compliance implementation, meaning the process and tools to track, evaluate, distribute and report on changes in laws and regulations and on emerging risks; (ii) data from the business and compliance; and (iii) annual risk-based compliance plans.

Within this framework, special attention should also be paid to identifying the mission critical compliance risks for the organisation, and applying a consistent strategy for each of those risks. First, articulate the risk and its mitigating controls. Second, establish key risk indicators (KRIs) to illustrate how well (or how poorly) controls are working. Third, identify data and analytics to track actual performance against KRIs. Fourth, agree on a monitoring and oversight plan with the business and other control functions such as internal audit and risk management. Fifth, create a standard reporting template for senior leaders and the board. Finally, change compliance reports from 'activity' (what compliance has been doing) to 'impact' (is our programme working and is the company complying with the rules and managing its risks?).

Successful pre and post compliance also requires clarity and accountability about who is responsible for what – not just what compliance will do, but the respective roles of internal audit, risk management, business units and leaders, legal, finance and HR. Some companies use spreadsheets or even a responsibility assignment matrix (RACI) – detailing who is responsible, accountable, consulted and informed – to make this happen.

By ensuring the pre and post are well in hand, compliance will not only do what it does best in

any organisation, it will give its business partners what they are desperately looking for. When NAVEX Global in 2022 asked over 1000 compliance and risk management professionals what was most important about their roles to their organisations' decision making, 86 percent responded "keeping my organization compliant with all relevant laws, policies and regulations" and 80 percent said "identifying, monitoring, mitigating and controlling risks to my organization".

There is one more critical, added benefit from this approach to compliance. Leaders of every organisation are rightly proud to say: "We do business the right way. We treat our customers, employees and communities fairly and honestly. We act with ethics and integrity and play by the rules." Getting the pre and post right will enable compliance to reinforce these commitments, surface and fix those instances where the company is falling short, and arm senior leadership with timely, relevant and actionable intelligence about the most pressing issues of the day. R&C

Jay M. Cohen
Of Counsel
Giordano, Halleran & Ciesla
T: +1 (732) 741 3900
E: jcohen@ghclaw.com

PERSPECTIVES

COMPLIANCE MEETS THE ARTS

BY **PATRICK HENZ**

According to Nacho Abia, chief operating officer (COO) of Olympus Corporation, "Compliance is more art than science". What could he have meant by this? To be sure, if we reduce the compliance function to its basics, it is all about complying with law. As a first step, the ruling law must be identified and internal regulations and processes created to inform employees what is expected of them. For various reasons, such as inexperience, ignorance or criminal intent, a certain number of employees may not follow the regulations. Inexperience can be countered by training, ignorance with dialogue, and criminal intent with effective controls.

Unfortunately, boundaries are not always visible, and attitudes may shift; if not adequately addressed, inexperience may turn into ignorance, or into criminal intent. It is up to the company, through its compliance office, in combination with other functions, to avoid this outcome. Ignorance can only be eliminated by a clear system, where humans and processes go hand-in-hand.

Topics like anti-corruption, free markets and sexual harassment, for example, should be easily understood by employees based on education, values and attitudes. These are basic rules for living in a society and part of being human. Nevertheless, since these problems do arise within organisations,

it shows there is a risk that individuals can 'unlearn' being human.

Section 8B2.1 of the Effective Compliance and Ethics Program of the 2021 United States Sentencing Commission Guidelines Manual, states that a "compliance and ethics program shall be reasonably designed, implemented, and enforced so that the program is generally effective in preventing and detecting criminal conduct. The failure to prevent or detect the instant offense does not necessarily mean that the program is not generally effective in preventing and detecting criminal conduct." Of course, 'reasonable' is the relevant word here and its meaning up for debate. Reason aligns with logic and knowledge. An undisputed and efficient risk assessment is required, then the identified risks must be measured and addressed, meaning eliminated, lowered, accepted or insured. Depending

on the probability and impact of risks, a "reasonably designed" compliance and ethics programme is expected. As digital transformation advances, companies that face higher risks are expected to adopt artificial intelligence (AI), such as machine learning, tools into their programme. In addition, the existence of psychological biases and ethical blindness mean that the compliance and ethics function must include behavioural science. Since bureaucracy and automation carry the risk that employees will become 'robotised', it is imperative for compliance and ethics to keep them human, so they do not lose their capacity for critical thinking.

To ensure effectiveness, a 'silo mentality' must be avoided. Internal processes must be as strict as necessary to address the needs and underlying risk – but no more, as bureaucracy demotivates employees, especially if processes are not understood. On another level, human nature must be considered when designing tools and processes: 'ethics by design'.

Singer and artist David Byrne argued that "In order to really succeed… you have to be able to think outside the box and do creative problem solving… creative thinking is in the arts". Arts has been included in schools and universities to enhance the classic science, technology, engineering and maths (STEM) to science, technology, engineering, arts and mathematics (STEAM) or even science, technology,

"Ignorance can only be eliminated by a clear system, where humans and processes go hand-in-hand."

reading, engineering, arts and mathematics (STREAM), underlying the importance of philosophy and reading. The Stanford Encyclopaedia of Philosophy defines art as part of human culture, but also an object of discussion. Art can please but also challenge observers, pushing them out of their comfort zone, confronting them with new ideas.

Consequently, art should not be limited to the chief executive's office or the boardroom, but spread to all work environments, including factories, workshops, offices and home offices. Aligned with corporate and local culture, art can be used to communicate corporate values, to artistically interpret them.

Art can be everything from fine art to street art, appealing to employees at all levels.

The ethics and compliance department can include art in its communication and training to push employees out of their mental comfort zones and keep them thinking, for example using cognitive dissonance to illustrate the connection between wrong decisions and consequences, or to highlight and deconstruct stereotypes and prejudices. In the best case, ethics and compliance dialogue should surprise participants.

Dissonance between the message and the expression of the message should spark cognitive processes, to try to understand the perceived gap. For example, the 1980s classic 'Enola Gay' by 'Orchestral Manoeuvres in the Dark' is on the surface an uplifting electronic dance tune but includes lines such as "this kiss you give, it's never gonna to fade away" and "is mother proud of little boy today?". Listeners may assume a romantic theme, unless they are aware that 'Enola Gay' was the name of the Boeing B-29 bomber which dropped the atomic bomb (nicknamed 'Little Boy') on Hiroshima. The interpretation of the song changes completely, and hopefully sparks an interest in this part of history. Ethics and compliance departments want employees to achieve compliance not because it is the rule, but because they understand the underlying connections. R&C

Patrick Henz
Head Governance, Risk & Compliance
E: cerpheus27@gmail.com

PERSPECTIVES

THIRD PARTY ANTI-BRIBERY AUDITS IN THE PHARMACEUTICAL SECTOR

BY **CHRISTOF STOLLA, PARAMES SUWANSIRI AND SOPHIA GEORGE-SEALY**
> NOVARTIS

The pharmaceutical industry, like many others, relies on third parties throughout its product lifecycle, from clinical research to manufacturing, marketing, promotion and distribution.

One area that is most scrutinised by regulators is third-party management – in particular for those third parties which are engaged in promoting or selling products, i.e., those who interact with patients and healthcare professionals. Over the past decade, more than 90 percent of enforcement actions executed by the US Department of Justice (DOJ) under the US Foreign Corrupt Practices Act (FCPA) involved third parties.

The FCPA, which also applies to foreign companies with securities traded on a US exchange or to other companies under certain circumstances depending on the US nexus of the transaction in question, is the primary US anti-bribery law.

In 2020, the DOJ published guidance on how it evaluates the effectiveness of corporate compliance programmes, setting out expectations and guiding principles. With respect to third parties, the guidance encourages companies to engage in ongoing, risk-based and proactive risk management of third parties throughout the life of the relationship.

Meeting these expectations poses unique challenges. How can companies understand and

evaluate the ethical business conduct and practices of independent third parties and identify potential risks, while respecting antitrust and competition principles? Once risks have been identified, how can these risks be remediated while protecting the independence of the third party? Finally, how can organisations encourage third parties, some of which are large and influential, to make investments to strengthen their compliance and risk management capabilities?

This article will cover a tool – third party anti-bribery audits – which, in our experience, can not only lead to direct and effective risk mitigation of third party compliance risks but also strengthens relationships with third-party partners and demonstrate the organisation's commitment to ethical business performance.

> **"Managing third parties is and will remain a key focus area for companies that are serious about compliance, as well as a key risk area with high scrutiny from external regulators."**

Elements of an effective third-party anti-bribery audit and remediation process

Before examining the key success factors for deploying third-party anti-bribery audits as a tool for the management of third party relationships, certain operational elements should be in place. These are: (i) a contract with an explicit right to audit; (ii) a risk-based third party selection criteria, (iii) a clear audit scope and focus, tailored to the type of relationship and activities of the third-party interaction; (iv) a consistent company-wide approach and process; and (v) an approach for collaborative remediation.

Key success factors for implementation of a third party anti-bribery audit and remediation process

Organisational buy-in and awareness. In our experience, communication of third party anti-bribery audits across multiple functions, including commercial, legal, compliance and internal audit, is critical to generating awareness and obtaining buy-in to the process. This, in turn, enables the successful operation of third party anti-bribery audits.

End to end engagement of primary third party relationship owners. It is critical that the primary relationship owner with the third party, such as a commercial team, is fully engaged in the entire

process as the main face of the company with the third party. In our experience, it is only the primary relationship owner who possesses the level of influence with the third party necessary to both educate the third party of the value of the audit process and keep them accountable to fulfil audit requirements and remediate identified risks. Some key roles of the primary relationship owner include explaining the value of the audit (ideally during the contract signing), removing any obstacles during the audit, and ensuring timely and high-quality remediation.

Agreeing to expectations of compliance within contractual clauses. It is key that every contract compels a third party to maintain proper books and records, includes a right to audit those books and records, and defines clear expectations of compliance. It is also important that every relationship owner of a third party ensures that the third party understands the existence and importance of such clauses. Organisations may opt to establish standardised clauses, and if any deviation is planned, there should be a process requiring endorsement by anti-corruption experts, such as legal, to ensure that suggested deviations do not prevent or limit the execution of audit rights.

Engage external audit providers to execute audits. Effective audits typically require uninhibited access to confidential information. Using an external audit firm bound to confidentiality can alleviate any third party concerns regarding access to confidential information and avoid inadvertent access to competitor data, such as product prices and commercial strategies which may potentially breach antitrust and competition requirements. Any external provider must also have knowledge and expertise of FCPA requirements, local pharmaceutical and healthcare compliance practices, and a global presence. As external audit firms typically serve many organisations and industries, they can also provide useful insights into common practices to inform the remediation process. Organisations should also collaborate with audit firms. Finally, as external audit firms are for-profit organisations, the company is advised to contact several for a quote, to obtain the best value for money while safeguarding the organisation from third-party risks.

Invest sufficiently for success. To the extent possible, and based on organisational footprint and structure, upfront investment in and allocation of resources to ownership of the third party anti-bribery audit process brings many benefits. Centralisation ensures consistency of third-party selection, audit approach and the important reporting and remediation stages. Central ownership is also less likely to be influenced by 'business interests', treating observations and audit outcomes with an objective eye, and will not cut corners when it comes to observations which need to be addressed. Preferably, associates working in this central team will have a compliance or audit background, can challenge the processes of external audit firms and possess good stakeholder-influencing skills.

Apply a standardised and objective process and approach. Each audit should follow a standardised process, which defines clear roles for the company, as well as the external audit firm. Clear criteria for risk rating an observation and remediating it should be defined, as well as clear reporting requirements and templates to ensure consistency across audits, even where different audit firms are being used.

Obtain third party and business input into audit results prior to concluding an audit. The third party should be able to provide management comments, as this will ensure there are no misunderstandings and will provide a good indication of whether a third party is willing to accept and later remediate certain

risks. Every draft report should be reviewed carefully by global and local teams, to ensure there is consistency and understanding of the risk rating and remediation approach, and to avoid any inaccuracies within the report.

Remediate promptly and collaboratively. Conclusion of an audit marks the beginning, not the end, of the process of risk reduction. It is important that remediation begins with a thorough review of risks identified in the audit and prioritises remediation actions. Ideally, this would be done directly and collaboratively in a meeting between the business relationship owner and the third party, to ensure full alignment on the remediation plan. Once a remediation plan is aligned, it is a good idea to formally document it in a letter outlining agreed actions, due dates and evidence to verify completion, and to have both parties countersign it to demonstrate mutual consent. Finally, all actions should be verified through a review of evidence to provide sufficient assurance that the risks have been addressed.

Conclusion

Managing third parties is and will remain a key focus area for companies that are serious about compliance, as well as a key risk area with high scrutiny from external regulators. A well thought out and consistently executed third party anti-bribery audit programme can lead not only to direct and effective risk mitigation of third party compliance risks, but also strengthen relationships with third-party partners as both organisations demonstrate their collective commitment to ethical business performance. R&C

Sophia George-Sealy
Director, Third-Party Anti-Bribery Audit
Novartis Ireland Limited
E: sophia.george-sealy@novartis.com

Christof Stolla
Global Head Review, Monitoring & Remediation
Novartis International AG
E: christof.stolla@novartis.com

Parames Suwansiri
Head of Enterprise Risk Management
Novartis International AG
E: parames.suwansiri@novartis.com

HOT TOPIC

ANTI-CORRUPTION COMPLIANCE AND INVESTIGATIONS IN HIGH-GROWTH MARKETS

PANEL EXPERTS

Neil Donovan
Senior Associate
Ashurst
T: +44 (0)20 7859 3238
E: neil.donovan@ashurst.com

Neil Donovan is a senior associate in Ashurst's dispute resolution practice. He specialises in global criminal and regulatory investigations. He acts for financial institutions and corporates across a range of sectors, including energy and natural resources, transportation, manufacturing, consumer goods and telecommunications. He has particular expertise in corporate crime matters and has completed a secondment to the Serious Fraud Office. He has acted for clients on multijurisdictional investigations related to allegations of bribery and corruption, money laundering, tax evasion and accounting fraud.

Glenn Pomerantz
Partner
BDO
T: +1 (212) 885 8379
E: gpomerantz@bdo.com

Glenn Pomerantz is a BDO partner with more than 35 years of forensic accounting, auditing and consulting experience and leads BDO's Global Forensic Practice. He is a certified public accountant and certified fraud examiner specialising in fraud investigations compliance and due diligence as well as domestic and international dispute resolution. His experience includes hospitality, gaming and restaurant expert witness, insurance claim and investigative matters for hotel owners, developers, investors and operators including with casino, food and beverage and golf operations. He has performed similar work for independent restaurants, food service providers and entertainment venues.

Hayley Trahan-Liptak
Associate
K&L Gates LLP
T: +1 (617) 951 9148
E: hayley.trahan-liptak@klgates.com

Hayley Trahan-Liptak is an associate in K&L Gates' investigations, enforcement, and white-collar practice group. Her practice focuses on government investigations, regulatory enforcement actions, internal investigations, white-collar defence and complex civil litigation matters. She represents public companies, individuals, investment advisers and financial institutions before various state and federal regulators and enforcement authorities, including the Securities and Exchange Commission (SEC), the US Department of Justice (DOJ), and the Financial Industry Regulatory Authority (FINRA).

R&C: How would you characterise corruption risks for companies operating in high-growth markets? In what ways have these risks evolved in recent years?

Donovan: For multinational companies, operations in high-growth markets are frequently managed or organised through subsidiary entities or joint venture partners. This increases third-party risk, as UK-based executives are removed, both geographically and structurally, from employees, service providers and customers on the ground in high-growth markets, which, in turn, makes effective oversight and due diligence all the more important. In high-growth markets, the frequent involvement of politically exposed persons (PEPs) and other government officials in bid, procurement or contracting processes remain a significant corruption risk. The enforcement risk for corruption has also significantly increased as governments globally, including in high-growth markets such as Brazil, have introduced strict anti-corruption laws and resourced local law enforcement agencies to pursue cases of suspected corruption.

Trahan-Liptak: Companies operating or expanding into high-growth markets have always had to be keenly aware of corruption risk. Such markets often lack robust anti-corruption protocols or a compliance culture, making it challenging for companies to expand without engaging in illegal practices. The current geopolitical climate has exacerbated many of these tensions. For instance, efforts to evade new Russian sanctions are on the rise, and increased inflation and cost of living have made people more susceptible to corruption and made spotting inflated payments more challenging. Reduced oversight of employees and vendors as part of pandemic-era policies has also contributed to corruption risks. Not only is the risk of corruption high in such markets, but the prevalence of corruption risk has also invited the US government to turn the spotlight on those areas. Last year, the Biden administration released the National Security Study Memorandum, announcing that combatting corruption would be a major strategy in protecting national interests. Viewing anti-corruption as a matter of national security is likely to lead to aggressive investigations and prosecutions by the US Department of Justice (DOJ). High-growth markets, which often pose their own risks to US interests, are likely to be a focus.

Pomerantz: Fraud and corruption risk in high-growth markets may be driven by several factors, including a burgeoning industry such as cryptocurrency, new technology such as artificial intelligence (AI), new and unfamiliar reporting structures such as environmental and social governance (ESG), or political opportunity and

pressure. In these markets, profits may lag revenue growth while internal controls, structures and governance may lag the infrastructure behind sales, marketing, recruiting and acquisitions. Decentralisation augments corruption risks in these high-growth markets with mature governance structures often decoupled from operation centres. Corruption risks tend to spiral out of control, get addressed and mitigated to a degree, then lapse when complacency sets in and political and legislative focus wane. Anti-corruption efforts must be a consistent, long-term, unwavering priority to remain effective in high-growth markets.

R&C: To what extent is geopolitical instability and the ongoing impact of the coronavirus (COVID-19) pandemic intensifying pressure on companies to grow and, in turn, fuelling instances of corruption?

Trahan-Liptak: Instability, whether it is caused by recession, lockdowns, geopolitical conflict or disease, often exposes corruption. Unscrupulous parties look to take advantage of instability, whether propagating new schemes or expanding existing activities in the absence of oversight. We saw this in 2020 when newly formed companies scrambled to import false coronavirus (COVID-19) products or personal protective equipment (PPE), or when fraudsters took advantage of government support programmes. For companies with an established corporate presence, COVID-19 lockdowns and work from home policies resulted in additional employee autonomy with limited oversight from managers. An impending recession may also lead companies to cut back on oversight roles. With minimal oversight, unsupervised employees may be more willing to take risks, and corruption may go unnoticed. As we saw during the pandemic, financial crises may also create incentives for employees to take or offer a bribe.

Pomerantz: Instability in any form diverts attention, allowing fraud and corruption the opportunity to flourish. During the COVID-19 pandemic, the fight against corruption faced unique hurdles as remote work replaced the traditional work environment. Corporate leaders had to adjust to the realities of working from home, including how to mentor, train and conduct oversight. Governments responded to the pandemic with unprecedented spending, inadvertently increasing the risk for fraud, abuse and corruption. Likewise, political instability, including the war in Ukraine, has created opportunities for bad actors as funding efforts have scaled. Companies must remain vigilant in this environment. In addition, corporate government assistance, sanctions compliance and ESG compliance are newer or evolving reporting

structures that must be evaluated with a watchful eye. Companies must apply both traditional and customised anti-fraud and corruption controls to mitigate these developing risks.

Donovan: Geopolitical instability and the ongoing impact of the COVID-19 pandemic, including supply chain pressures, high rates of global inflation and the cost of living crisis, are all intensifying pressure on companies and creating an environment ripe for corruption. Companies and employees are increasingly being forced to seek alternative ways of maintaining growth and winning new business in a depressed market, with staff in sales and business origination roles often pushing legal and ethical boundaries to meet targets. We expect kickbacks, facilitation payments and opaque payment flows to increase as companies seek to artificially maintain profit levels and achieve commercial objectives.

R&C: What considerations should be top of mind for multinational companies seeking to avoid breaching anti-corruption laws?

Donovan: The level of political and public appetite globally to tackle corporate corruption should not be underestimated or ignored by companies. Anti-corruption is a topic which falls squarely within the social and governance limbs of governments' ESG agendas. As a result, companies can expect significant reputational damage and adverse publicity in the event they are exposed to a corruption investigation or enforcement action, in addition to large financial penalties. This, in turn, can have a detrimental effect on share price, impact employee morale, and lead to follow-on litigation against the company by competitors and stakeholders who consider they have suffered a loss as a result of the company's actions. A strong compliance culture which permeates

> **"Communicating and actively demonstrating a zero-tolerance approach to corruption is integral to ensuring compliance among the workforce."**
>
> *Neil Donovan, Ashurst*

through company structures and business lines, effective training, clear and practicable policies and procedures, including robust due diligence checks, and secure escalation channels, are critical controls for companies seeking to avoid breaching anti-corruption laws. For multinational companies, it is important that controls are fit for purpose across the geographical regions in which they operate and are tailored to meet standards of local laws and best practices.

Pomerantz: Multinationals should approach anti-corruption laws from a 'do what is right' perspective. Laws and regulations are designed to prevent and mitigate corruption by discouraging inappropriate behaviour. There are few exceptions to anti-bribery laws and regulations, so playing by the spirit of the law is always the best course of action. Even then, diligence across the organisation is needed. Despite world-class training, superior internal controls, and vigilant third-party vetting, a rogue employee can cause significant damage to a strong infrastructure of preventative corruption controls. Companies must assume potential breaches of anti-corruption controls and conduct substantive anti-corruption testing, which includes designing, implementing and regularly monitoring transactions, journal entries, relationships and margins.

Trahan-Liptak: An established and effective compliance programme is the best way to comply with anti-corruption laws, to identify breaches, and to help reduce or avoid potential penalties following a violation. The DOJ Justice Manual provides a comprehensive overview of what prosecutors must look for when evaluating a compliance programme and provides excellent guidance for companies looking to develop and maintain an effective programme. The Justice Manual outlines three fundamental questions for evaluating a compliance programme, including if the programme is well designed to detect the types of misconduct that may occur in the company's business and operating location, if it is 'adequately resourced', and if it works in practice. As a first step in ensuring a compliance programme is effective and will

> **"The calculus driving trends in corruption in high-growth markets is often dependant on economic circumstances and political attitudes toward corruption."**
>
> *Glenn Pomerantz, BDO*

stand up to such scrutiny, multinational companies should be attuned to evolving risks that are inherent in each of the jurisdictions where they operate, understanding that different jurisdictions will pose unique risks.

R&C: What steps should a company take to raise awareness of and commitment to anti-corruption compliance among its workforce? How important is regular, focused and engaging training?

Pomerantz: Awareness, commitment and training are perhaps the most discussed anti-corruption topics. The DOJ, US Securities and Exchange Commission (SEC), the Organisation for Economic Co-operation and Development (OECD), the Serious Fraud Office (SFO) and numerous additional regulators and law enforcement agencies provide guidance and suggestions on employee anti-corruption awareness and commitment. However, corporate compliance programmes do not always account for factors outside the company. Corruption can often emanate from complex collusive schemes involving business partners, distributors, agents, suppliers and customers. Training and vetting the people outside of an organisation who interact with employees can be just as important as employee anti-corruption awareness and training. Providing avenues for third parties to report fraud and corruption and not limiting these channels to employees can contribute to the breadth and depth of anti-corruption awareness and enhance leadership's ability to mitigate fraud.

Trahan-Liptak: Developing a culture of compliance can be challenging, particularly in emerging markets where there are existing limited controls. Regular training sessions are an important part of creating this culture. The DOJ Justice Manual calls training a "hallmark" of a well-designed programme, and requires prosecutors to assess whether the company has integrated its policies and procedures through trainings of relevant parties. Training sessions, like the compliance programme itself, must be adapted to the audience. Training sessions for employees in high-growth markets should be tailored to the risks present in the jurisdiction, just as training for employees and gatekeepers must address the employee's responsibilities and risks in their field and geographic area. Such training schemes will help reduce corruption risk and may lead to more favourable resolutions if failures do occur. In addition to training programmes, local and global management must set the tone of compliance from the top.

Donovan: Tone from the top is a key component of effective compliance programmes. A central pillar of this is fostering a compliance culture that is cascaded by senior management throughout the business. Communicating and actively demonstrating a zero-tolerance approach to corruption is integral to ensuring compliance among the workforce, including third parties performing services on behalf of the company. Based on the size and breadth of a company's operations, establishing a designated committee with responsibility for oversight of anti-bribery and corruption is also an effective way to monitor the effectiveness of the compliance programme on an ongoing basis. Training is an important way of supplementing a tone from the top message by ensuring employees and contractors are suitably informed of applicable anti-corruption laws, equipped to identify typical indicators of corrupt activities, and understand what steps they should take to escalate concerns. Training should be delivered to all employees and contractors when they join the company and refreshed on an annual basis. Enhanced training should be provided to individuals in higher risk roles which is bespoke to the risks of their business, such as procurement or sales.

R&C: How important is it for companies in high-growth markets to carry out effective auditing and due diligence processes as part of their anti-corruption efforts?

Trahan-Liptak: Conducting due diligence of vendors, agents and other third parties prior to an engagement will help companies avoid entanglements with bad actors. To be effective, companies must tailor the scope and method of due diligence to the operating jurisdiction. For example, online reviews of vendors may be sufficient diligence for some US contractual relationships, but in markets where companies have limited internet presence or governmental oversight is limited, the same searches may be insufficient to make an informed decision about contractual partners. Regular, ongoing due diligence, even after the start of a contractual relationship, can help identify if the same parties are still in control or if new facts about the third party have emerged. The routine monitoring of policies, procedures and contracts are also essential in identifying problems before they get out of hand.

Donovan: One of the principal means by which companies can avoid corruption risks is through robust due diligence processes in relation to their domestic and overseas operations, specifically in relation to third parties that they engage to perform services. Third-party due diligence is particularly important given companies can be liable for the acts of third parties under anti-corruption legislation, including the UK Bribery Act 2010. Supply chain and third-party audits should be conducted periodically, and related risk assessments should be refreshed to align with a company's risk profile as it evolves. Taking a proactive approach to due diligence will enable companies to identify and mitigate corruption risks before they crystallise.

Pomerantz: Strong forensic auditing and comprehensive due diligence procedures can be a safety net for anti-corruption programmes. Companies, with the assistance of advisers, have developed sophisticated and effective forensic audit tools to help combat corruption. These tools include data analytics, AI, automated journal entry testing and other means for conducting substantive testing of transactions, balances and agreements, as well as other unstructured and structured data. These substantive forensic accounting procedures are paramount in higher risk geographies where actors with a history of illicit behaviour permeate and unabashedly design and conduct collusive fraud and corruption schemes that put a global company's reputation at risk. A combination of well-designed fraud and corruption controls, which include training and robust substantive testing based on identifying

patterns of unusual transactions, relationships and balances can be the most effective mechanism for mitigating these very real fraud and corruption risks.

R&C: What advice would you offer to companies on strengthening their internal controls to detect and respond to potential corrupt activities? Where do reporting mechanisms and whistleblower protections fit into this equation?

Pomerantz: Two significant controls are often non-existent or often break down, allowing common fraud and corruption schemes. One is segregation of duties. A large proportion of fraud and corruption schemes may occur because a bad actor is left unchecked with too much authority over too many areas of the business. Contract approvals, bid analyses and determinations, pricing decisions, use of offshore accounts, and use of intermediaries are all critical decisions that should have built-in initiator and approval redundancies allowing for proper segregation of duties to mitigate the likely fraud and corruption schemes. Reporting mechanisms and non-retaliation policies also play a significant role in a company's anti-fraud, and anti-corruption cache. Many reputable studies conclude that the number one mechanism for identifying schemes is tips from employees and third parties. Companies that build these protections into their policies, code of conduct and culture position themselves to reap the benefits of an important and reliable mechanism for reporting fraud and corruption.

"Companies should consider the scope of the allegations, if the investigation should remain privileged, and the nature of risks the investigation may uncover."

Hayley Trahan-Liptak, K&L Gates LLP

Donovan: Effective oversight and regular testing of controls to ensure they are calibrated to detect the risks specific to the company's business is key. For companies operating in high-growth markets, this is particularly relevant to subsidiary oversight and the need for senior management to be aware of the specific risks that might impact operations overseas. Group-level policies are, if properly implemented and periodically reviewed, an effective way of ensuring a consistent approach which meets

global standards of best practice. These group-wide policies should be supplemented at an in-country level to reflect specific legislative or regulatory requirements related to anti-corruption. Effective whistleblowing channels, for both internal and external reporting, ensures that risks or wrongdoing within the business are identified and escalated as quickly as possible. The effectiveness of internal reporting channels will ultimately depend on whether they provide the necessary safeguards to encourage employee engagement, including protections from retaliation and measures to maintain the anonymity of reporters.

Trahan-Liptak: On the ground, employees are a company's best asset when it comes to avoiding, identifying and preventing compliance failures, but only if they are well trained and given the resources to identify and report corruption. Companies can start employees on the right track by fostering a compliance environment, requiring regular training, setting and discussing policies, and encouraging reporting. From there, companies should provide employees with the necessary tools to act if they see risks in their everyday work. Well-advertised reporting hotlines, frequent and open communication with the compliance team, and documented whistleblower protection resources will encourage employees to come forward if they do identify risks. Finally, companies must act swiftly to discipline any employees or vendors engaged in corruption. Failure to make an example out of wrongdoers risks reversing all of the progress the company has made when setting the tone for compliance.

R&C: If a company does receive reports of potential corruption within its ranks, how should it prepare for and carry out an internal investigation?

Donovan: The first step in any investigation should be a scoping exercise to identify the scale of the issue and the nature of investigative work required. This will include identifying the relevant parties, jurisdictions and the period of suspected wrongdoing. It is also important to consider how the investigation will be resourced, including whether external advisers are required, and any reporting obligations, such as to external authorities, law enforcement, insurers or other contractual notifications. Consideration should also be given at the outset to whether the investigation should be conducted on a legally privileged basis and steps taken to protect a company's claim to privilege. Once a clear scope has been established, documentary evidence that may be relevant to the matters being investigated should be preserved. Document preservation notices should be sent to all relevant parties and routine data deletion

procedures should be paused. A typical internal investigation follows a three-stage lifecycle: data and document review, interviews with relevant parties, and reporting on findings. Conducting a data review at the outset is the principal means by which the scale of the issue can be determined, and documents identified to test interviewees' knowledge, understanding or potential involvement in the suspected conduct. At the reporting stage, it is important to consider the target audience, be it internal management or external authorities, and whether the report may be disclosable, such as in any follow-on litigation proceedings.

Trahan-Liptak: Prior to beginning an investigation in earnest, the company should identify who will carry out the investigation. Companies should consider the scope of the allegations, if the investigation should remain privileged, and the nature of risks the investigation may uncover. For example, allegations of payments to government officials, which implicates the FCPA and suggests a government investigation could follow, would weigh in favour of an investigation run by the legal department or outside counsel. On the other hand, reports of inappropriate use of funds that are not linked to bribery may be more appropriately handled by the internal audit or human resources teams. Regardless of who is managing the investigation, the company should begin by collecting and preserving evidence, especially if a future government investigation may follow. Whoever is leading the investigation should then work with employees to discover all the relevant information.

Pomerantz: First, investigative planning should not wait until reports of potential corruption occur. Companies should design investigative policies and protocols as part of their compliance strategies. Upon receipt of a credible report of fraud or corruption, a preliminary review and verification of the allegation should be conducted. An assessment may guide the company on its notification decisions including notice to auditors, insurers, regulators, business partners and other stakeholders. Once a credible allegation has been made, mitigation strategies should be executed, like the capture of relevant data, both electronic and paper, and the isolation of the accused. The legal team assigned to the investigation will need to make decisions on disclosure, data privacy and the breadth of the investigation. Ultimately, the investigation will evolve into its final phase, including the remediation of control weaknesses, possible termination of employees and other business relationships, training enhancements and other remedies. Companies should strive to take meaningful action quickly to demonstrate the commitment of company

leadership to a fraud-free environment and to avoid harsh repercussions.

R&C: Do you expect corruption risks for companies in high-growth markets to intensify in the months ahead? Is it essential for companies to keep anti-corruption compliance near the top of their risk management agenda?

Trahan-Liptak: As economies around the world dip toward recession, following a period of two years of reduced oversight, the risks for companies operating in high-risk jurisdictions are particularly pronounced. Not only are companies likely to see reductions in staff, but management is likely to be distracted by surviving in a challenging economy. This leads to an environment ripe for corruption, particularly as third parties and some employees may be more willing to engage in corruption as inflation rises and the economic outlook grows dim. Companies should remind themselves that continued monitoring of risk and adherence to compliance protocols, even in the worst of times, will pay dividends in the long term by helping companies avoid expensive investigations and penalties.

Pomerantz: The calculus driving trends in corruption in high-growth markets is often dependant on economic circumstances and political attitudes toward corruption. In high-growth markets, economic expansions present greater business opportunities with increased temptation for corruption while recessions bring lower profits and desperation if a company's existence is threatened. With a potential recession on the horizon, fraud and corruption risks will grow. Company compliance departments have their plates full. Tomorrow's fraud and corruption risks and schemes are unlikely to be similar and certainly not identical to those of the past. The next wave of fraud and corruption is already here in the digital asset space and ESG. What lies ahead no one knows, but some new form of fraud and corruption is certain.

Donovan: Geopolitical instability, the ongoing impact of the pandemic, and global economic uncertainty are all factors which are likely to increase corruption risks for companies in high-growth markets, particularly in emerging markets, in the months ahead as competition intensifies and companies push ethical boundaries to meet shareholder and customer expectations. Against this backdrop, there remains clear political and public appetite to intensify the spotlight on anti-corruption enforcement, which means it must remain a priority agenda item for management. Companies can expect the introduction of new anti-corruption laws, increased resourcing of law enforcement

agencies tasked with investigating and prosecuting corruption, and greater cooperation between global authorities. The overlap between anti-corruption and ESG considerations is another factor which we anticipate will continue to shape the anti-corruption enforcement and compliance agenda. R&C

EDITORIAL PARTNER

SAS

www.sas.com

No matter what role risk plays in your organisation, **SAS** has proven methodologies and practices to help you meet regulatory demands with confidence. SAS' high-powered analytics empowers users to increase efficiency, transparency and profitability. Risk is at the core of banking, and SAS' seamless risk framework enables a risk-aware culture and optimises capital and liquidity. How do we know? SAS provides award-winning risk management to customers globally.

KEY CONTACTS

Sumit Chattopadhyay
North America Head, Risk & Finance Advisory
Cary, NC, US
T: +1 (919) 677 8000
E: engagementcenter@sas.com

Mingyuan Zhang
Principal Solutions Architect
Cary, NC, US
T: +1 (919) 531 4723
E: sunny.zhang@sas.com

EDITORIAL PARTNER

www.corporatecompliance.org

Society of Corporate Compliance and Ethics

Society of Corporate Compliance and Ethics (SCCE) is a non-profit, member-based association serving 6500-plus members in over 100 countries. Founded in 2004, SCCE is dedicated to supporting compliance and ethics professionals across all industries and promoting the lasting success and integrity of organisations worldwide. SCCE offers 45-plus educational conferences and 90-plus webinars a year, publications, training resources, and certification and networking opportunities to support practitioners as they grow in their careers and develop and maintain their compliance and ethics programmes.

KEY CONTACT

Robert Bond
Immediate Past President
London, UK
T: +44 (0)7880 892717
E: rtjbond@icloud.com