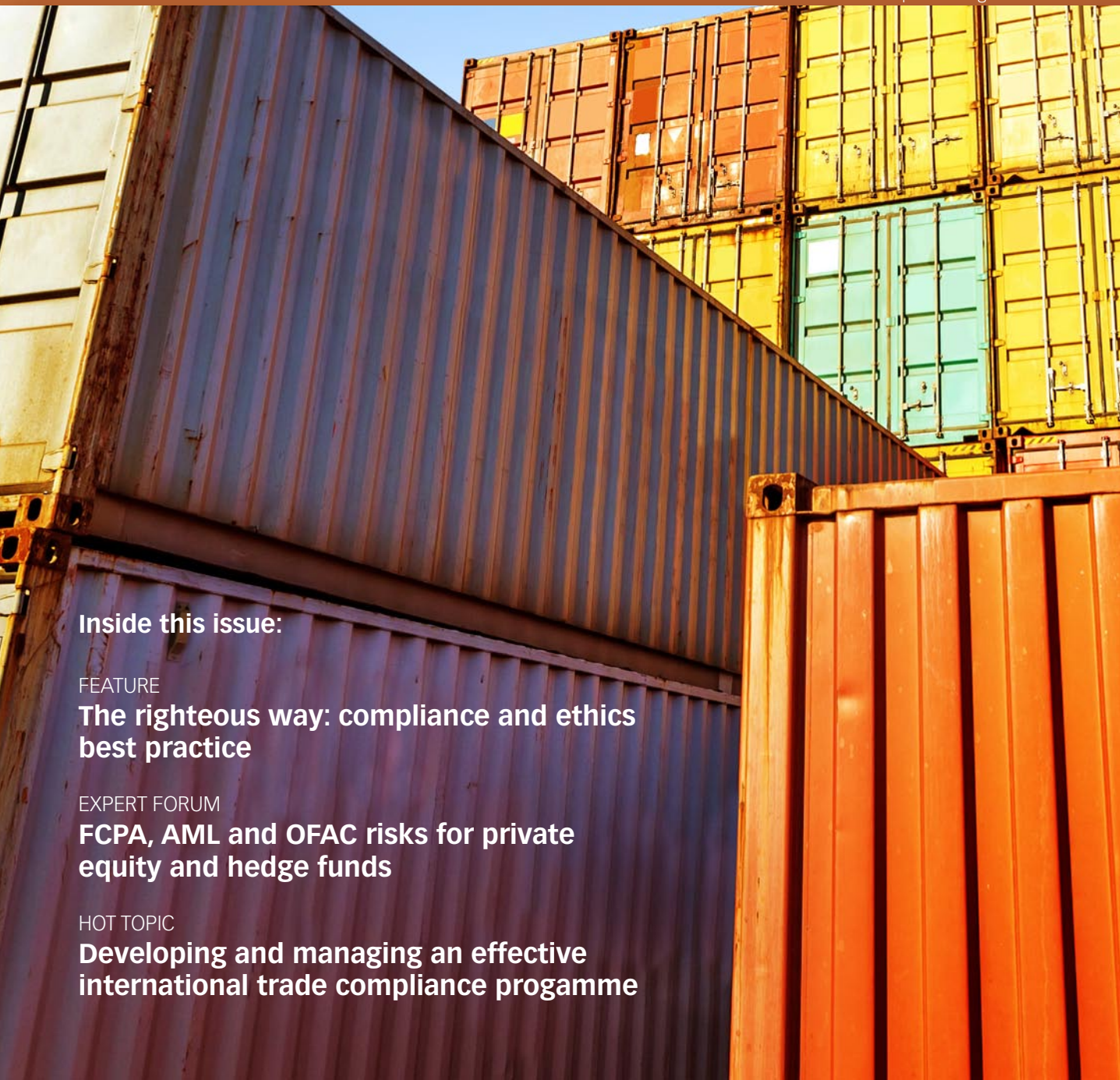
R&C risk & compliance

OCT-DEC 2016

www.riskandcompliancemagazine.com



Inside this issue:

Effectively Manage Third Party Risks with RISKRATE™

NAVEX GLOBAL®
The Ethics and Compliance Experts

Protect your organization against legal, reputational and financial risk with RiskRate:

- Automated Screening Process
- Continuous Due Diligence Monitoring
- Flexibility Where You Need It
- Optional Analyst-Driven Reports

Learn more about RiskRate today **www.navexglobal.com/RiskRate**

RISKRATE™
Enterprise Due Diligence

www.navexglobal.com | +1 866 297 0224 | info@navexglobal.com

R&C CONTENTS

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

Risk & Compliance
Published by Financier Worldwide Ltd
23rd Floor, Alpha Tower
Suffolk Street, Queensway
Birmingham B1 1TT
United Kingdom

+44 (0)845 345 0456
riskandcompliance@financierworldwide.com
www.riskandcompliancemagazine.com

ISSN: 2056-8975

Mind over risk:

The secret behind successful merger and acquisition deals and the people who insure them.

TOKIO MARINE HCC

As well as holding extensive experience and in-depth knowledge of worldwide transaction risk related issues, our dedicated transaction risk insurance team of underwriting, lawyers and claims specialists, offers a fast and efficient service. Being internationally focused means that, wherever you are based, we have the intelligence to help you close the deal successfully.

Transaction Risk Insurance: Warranty and Indemnity • Tax Indemnity • Contingent Risk Transfer

Torre Diagonal Mar, Josep Pla 2, 10th Floor, 08019 Barcelona, Spain
Tel: +34 93 530 7300 tmhcc.com

FOREWORD

Welcome to the sixteenth 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 compliance and ethics best practice and on tackling financial crime in the EU. We also look at: risks for private equity and hedge funds; third party and counterparty relationship risks; the Modern Slavery Act 2015; developments in RegTech; breaking the risk glass ceiling; reputation risk management; directors' duties and liabilities in Saudi Arabia; using Big Data and analytics; Basel III principles for risk data reporting; the new Privacy Shield; digital supply chains; employing ex-hackers for security purposes; transactional insurance; deal litigation; devices and data; human capital reporting; TSCA safety reform; liability for 'made in USA' claims; international trade compliance; and more.

Thanks go to our esteemed editorial partners for their valued contribution: AlixPartners; Ambridge Partners LLC; EY Advisory; FisherBroyles, LLP; IdentityMind; NAVEX Global; Paragon International Insurance Brokers Ltd; Richards Kibbe & Orbe LLP; Tokio Marine HCC; Walkers; Airmic; the Chartered Institute of Procurement & Supply (CIPS); the International Center for Compassionate Organizations (ICCO); ICSA: The Governance Institute; ISACA; and the WomenCorporateDirectors Education and Development Foundation, Inc.

– Editor

FEATURE

THE RIGHTEOUS WAY: COMPLIANCE AND ETHICS BEST PRACTICE

BY **FRASER TENNANT**

Despite the moral decrepitude which seems to pervade the world today, one would still like to think that most people desire to be essentially righteous when it comes to their attitudes, actions and behaviours. Of course, adhering to a set of moral principles is easier said than done – especially in a corporate context where such principles may have to sit within a vague framework of business ethics.

Yet for those companies that are committed to installing and sustaining a strong ethical culture across their business, having recourse to a robust compliance and ethics (C&E) programme is a key requirement. Such standards, procedures and controls can go some way toward preventing and detecting unethical conduct within the ranks. In addition, an effective C&E programme can also garner kudos externally, if a company is seen to be doing business 'the right way'.

According to Compliance 360, a C&E programme needs various facets. First, establish policies, procedures and controls. Second, exercise effective compliance and ethics oversight. Third, exercise due diligence to avoid delegation of authority to unethical individuals. Fourth, communicate and educate employees on C&E programmes. Fifth, monitor and audit C&E programmes for effectiveness. Sixth, ensure consistent enforcement and discipline of violations. Finally, respond appropriately to incidents and take steps to prevent future incidents. These

elements form the core of a C&E programme, and should be implemented throughout the organisation, from the shop floor to the decision-making upper echelons.

That said, many compliance consultants are surprised by the number of senior managers, including CEOs and general counsel, who are yet to fully buy-in to the idea of compliance and ethics. However, for those companies that do more than just pay lip service to a C&E programme, the positives – such as an enhanced workplace culture and less chance of a workplace lawsuit – greatly outweigh the negatives – such as the requirement for top level management support and cost and time factors – in virtually every scenario.

"The critical message is that compliance and ethics are fundamentally good for business," says Chris Rowley, director of the Risk Advisory Group. "A strong C&E programme is about ensuring businesses maximise returns by working in the right way, with the right people. Effective compliance should facilitate good business, not inhibit it. That is why it should be at the forefront of the decision-making process, not an afterthought – under-funded, under-respected and sometimes ignored altogether. Compliance and ethics isn't a passing fad. These have become fundamental issues which now sit at the apex of business success and stakeholder value."

Furthermore, with publication of a new anti-bribery management systems standard, called ISO 37001, expected by the end of 2016, the pressure being placed on companies to have in place an effective corporate C&E programme has never been more acute.

As one might expect, to successfully implement a workable C&E programme, there has to be a strong appetite to introduce such measures across the length and breadth of a company, not just in isolated pockets which would have little impact. In the view of Michael Volkov, CEO of the Volkov Law Group LLC, companies that are looking to build a robust C&E programme must base their plans on a risk assessment, and allocate available resources based on this risk assessment. "A one-size-fits-all approach will not work," he suggests. "Each company has a unique set of risks and market conditions that they need to consider in designing and implementing an effective C&E programme."

Risk mitigation

Unique risks, along with more general corporate risks such as supply chain losses, fraud such as asset theft, regulatory violations, corruption and bribery allegations, as well as issues relating to corporate responsibility, are reasons why implementing a C&E programme is deemed to be such a worthy addition to an organisation's armoury. But it also goes further. "An effective C&E programme can not only mitigate risks, but can create a corporate culture that increases financial profitability, sustainability and long-term growth,"

asserts Mr Volkov. "Research has shown over and over again that a positive culture of ethics leads to greater employee trust, productivity and sustainability."

For some experts, compliance and ethics is about choices. "Business is challenging, and to be successful in tough economic conditions, companies have to exploit opportunities in ever more complex, developing markets," says Mr Rowley. "But by having an agreed set of standards by which you will operate, by ensuring that you know exactly who you are doing business with, and by not taking short

cuts, a business is far better placed to succeed and avoid costly mistakes than if it risks everything for short term gain."

When it comes to compliance and ethics issues, there is also the not inconsiderable matter of personal risk to corporate leaders, who may be exposed to financial penalties, disbarment from holding office or even jail, should the authorities uncover unethical conduct of sufficient gravity.

Board buy-in

For a C&E programme to be successfully implemented throughout all levels of an organisation, it is necessary for a board to fully demonstrate its engagement with the compliance and ethics environment, perhaps even installing such issues as a regular item on the boardroom agenda.

"Boards are under greater scrutiny than ever before to demonstrate their commitment to compliance and ethics," points out Kristy Grant-Hart, managing director of Spark Compliance Consulting. "It isn't enough in this ever-increasing regulatory environment to simply nod toward compliance and ethics. Shareholders, regulators and the public at large are paying attention to corporate ethics like never before." She adds that boards need to pay particular attention to this critically important aspect of their responsibilities and invest in a proper C&E programme up front, instead of paying huge fines and dealing with public scrutiny and reputational harm and only then looking to implement a strong compliant and ethical culture.

Today, companies not only have to conduct their business with integrity, they also have to ensure that this conduct is easily demonstrable. "The board's commitment must go further than one of principle," says Philippe Montigny, president of Ethic Intelligence. "Certification of anti-corruption compliance programmes is a way to establish the board's commitment to the corruption prevention programme and demonstrates their genuine buy in."

Ignorance

For companies that routinely sideline or completely ignore the importance of adopting a compliance and ethics strategy, the consequences can be devastating. A multitude of troublesome scenarios lie in wait to irrevocably compromise future financial performance. "Firms that ignore the due diligence required are risking not only their personal reputation but also their employees, customers, corporate name, brand and goodwill," warns Phil Wilson, founder and architect of Member Services and Programs at GRC Sphere. "Management needs to 'wake up and smell the coffee'. If a compliance and ethics foundation-building roadmap is not in place, then management had better take immediate action and get it nailed down."

As well as the outward-facing consequences of failing to implement an all-encompassing compliance and ethics culture, such as fines, government

investigations, shareholder derivative suits, large legal bills, financial penalties, corporate monitorships and reputational damage, serious internal damage can be wrought. "The non-obvious consequences include lost employee morale, candidates who won't come work for your company because they don't want to be associated with your brand and an acceptance of the moral decay experienced by employees that comes from watching managers misbehave without consequences," explains Ms Grant-Hart.

Good for business

Given the vagaries of the ethical landscape, it seems a foregone conclusion that the various levels of management with primary responsibility for C&E programmes – including the board of directors, senior management and other individuals – will see their duties mount exponentially.

"The need for strong corporate culture is only going to continue to increase in importance," states Alisdair McIntosh, policy and external relations director at the Chartered Institute of Internal Auditors (CIIA). "Corporate scandals ranging from LIBOR rigging to the Volkswagen emissions debacle have underlined the need for strong organisational culture to rebuild confidence and trust in business. This much is clear to the regulators, with the Financial Reporting Council (FRC) recently releasing its own report on corporate culture, to which the CIIA contributed on the importance of embedding and assurance."

This report, entitled 'Corporate Culture and the Role of Boards', released in July 2016, explores the relationship between corporate culture and long-term business success in the UK. One enlightening aspect of the report is that internal audit has a key role to play in providing assurance to the board that its desired culture is being embedded and lived out in the organisation.

"Today, companies not only have to conduct their business with integrity, they also have to ensure that this conduct is easily demonstrable."

There is little doubt that compliance and ethics will continue to gain importance as regulations proliferate and penalties grow. "The proliferation of social media and the interest in responsible business, green initiatives and corporate brands mean that it is a competitive advantage for a company to be perceived as being focused on

corporate compliance and ethics," suggest Ms Grant-Hart. "Ethical business is good business. It is good for the shareholder, good for the employee and good for the world."

Ethical compliance is maintained for the benefit of the company and its employees, and, to a certain extent, to satisfy any scrutiny, regulatory or otherwise, that may come to pass. Not only can it result in a strong working relationship between staff and management, it can also reduce employee turnover, improve morale and have a positive effect on productivity – all major factors in the creation of an attractive workplace culture. To these ends, the virtues of a C&E programme that promotes ethical standards while enhancing the working environment should not be underestimated. R&C


EY
Building a better working world
If there's no reward without risk, can risk be a good thing?
Risk is a much more risky proposition than it used to be. Yet, while many organizations see risk as a negative, good risk management can actually help companies go faster.
Visit ey.com/advisory
The better the question. The better the answer. The better the world works.
© 2016 Ernst & Young LLP. All Rights Reserved. ED0617.

FEATURE

TACKLING FINANCIAL CRIME IN THE EU

BY **RICHARD SUMMERFIELD**

Tackling financial crime is one of the biggest challenges that security agencies, regulators and companies face today. Criminals are robust, resourceful and relentless. While efforts continue to diminish the effect that financial crime has on the global economy, criminals use increasingly sophisticated tactics to remain one step ahead of the authorities and firms. According to Special Inspector James Phipson, commercial director of the Economic Crime Directorate at City of London Police, financial crime costs more than $2.1 trillion globally.

Regulators and law enforcement agencies continue to fight back, but it often appears as if the criminals are winning. A report published by PwC in July indicated that in spite of "significantly increasing investment in compliance and being continuously under the scrutiny of regulators", economic crime in the global financial services sector has increased markedly in recent years.

The financial services industry is perhaps most threatened by economic and financial crime, given its role as facilitator of so much financial activity. Indeed, 46 percent of respondents in the financial services industry surveyed by PwC said they were victims of economic crime in the last 24 months – 10 percent ahead of the industry-wide global average.

Financial institutions are not neglecting their investment obligations in the fight against financial criminality, with compliance expenditure outstripping

other industries. But it is not enough just to throw money at the issue. Firms need a more holistic approach, which has been lacking in the past. As PwC notes in its report, "Financial services organisations have struggled to join the strategic dots across the growing volume, sophistication and variety of economic crime".

But tackling financial crime is not confined to the boardroom – efforts must also be made at a national and international level. The FATF Recommendations, issued by the Financial Action Task Force and taking in 198 nations worldwide, have established a wide-ranging framework of measures which countries should implement in order to combat money laundering and anti-terrorist financing. The recommendations have been designed to complement existing legal, administrative and operational frameworks. Given the diversity of these national frameworks, a blanket approach is not feasible, so the FATF recommendations must be adapted to suit national circumstances.

Though there have been global efforts to tackle financial crime, regional attempts have varied. The EU introduced the Fourth Anti-Money Laundering Directive (AMLD4), designed to update and enhance anti-money laundering (AML) and counter-terrorist financing (CTF) laws. AMLD4 will impose tougher AML/CTF regimes and help to break down national borders to compliance by establishing a central database of corporate ownership. It will increase scrutiny of domestic politicians and enhance reporting of suspicious financial activity.

"AMLD4 will impose tougher AML/CTF regimes and help to break down national borders to compliance by establishing a central database of corporate ownership."

Dr Jens H. Kunz, a partner at Noerr LLP, notes that one of the key features of AMLD4 is the emphasis on the risk based approach. "This ensures that obliged entities take adequate measures to prevent money laundering and financing of terrorism instead of pursuing a one-size-fits-all approach by applying specified rules. While certain member states like Germany have already broadly introduced this approach, other member states might have to materially adjust their statutory framework. Initially, this sounds as if the level of harmonisation within the EU could suffer, but this concern does not seem to be justified given the introduction of risk reports and guidelines for an appropriate risk assessment by

the EU Commission and the European Supervisory Authorities," he says.

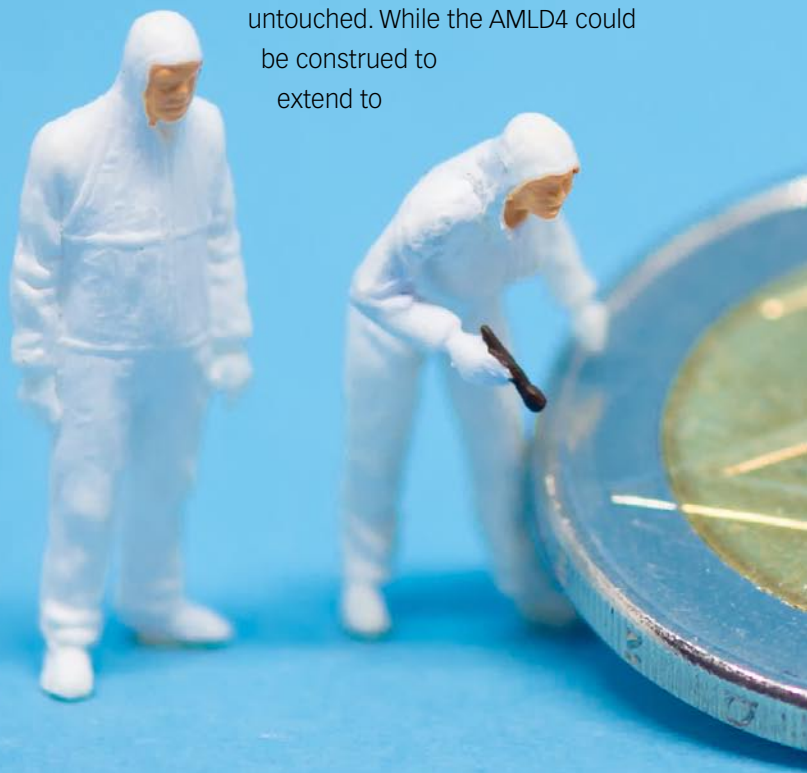
Matt Taylor, managing director at Protiviti, believes that AMLD4 underscores the global approach to tackling AML and CTF by aligning with the FATF Recommendations. "The Directive emphasises the risk-based approach, extends the scope to gambling service providers and now includes tax crimes as a predicate offence," he says.

The development and implementation of AMLD4 is a positive step, though its design will be an ongoing process. In July, the EU Commission published proposed amendments to AMLD4 to crack down further on terrorist financing, following the recent increased terrorist threat in the EU. The proposals seek to increase transparency by making beneficial ownership information public, and will affect companies and other legal entities, such as foundations and trusts.

Cryptocurrency

Cryptocurrencies, such as Bitcoin, have been an area of growth in recent years, and regulators and companies need to respond. Cryptocurrencies, and the blockchain technology on which many are built, have the potential to disrupt the financial services space (and many other industries) by removing the middle man.

According to a new report from the SWIFT Institute, however, the EU is still years away from implementing a consistent framework for cryptocurrency regulation. The introduction of new legislation, notably AMLD4 and the Revised Directive on Payment Services (PSD2), has done little to factor in the importance and relevance of cryptocurrencies. According to the Society for Worldwide Interbank Financial Telecommunication, the Directives "have not paid sufficient attention to this development, thus leaving virtual currencies largely untouched. While the AMLD4 could be construed to extend to



virtual currencies, the precise degree to which it will succeed in deterring their abuse for money laundering and terrorist financing purposes remains to be seen".

The EU has sought to respond to these concerns. In August, the European Commission (EC) proposed amendments to AMLD4 with the aim of creating a database of information on users of virtual currencies, linking users to their real-world identities. Such a move would effectively end the 'anonymity' feature which has been associated with digital currencies for long and which is a huge part of their appeal. But such anonymity has also facilitated illegal behaviour. "To combat the risks related to the anonymity, national Financial Intelligence Units (FIUs) should be able to associate virtual currency addresses to the identity of the owner of virtual currencies. In addition, the possibility to allow users to self-declare to designated authorities on a voluntary basis should be further assessed", notes the EC's proposals.

Dr Kunz confirms that while AMLD4 does not explicitly address virtual currencies, the EC proposal includes propositions to materially tighten the AML-framework in this respect. "The scope of AMLD4 shall be expanded to comprise, as obliged entities, virtual currency exchanges and providers of e-wallets which function as sort of gatekeepers for money laundering purposes in the context of virtual currencies. That means that those platforms and providers will have to apply customer due diligence controls when exchanging virtual for real currencies. This represents considerable progress and will address the concerns related to money laundering and terrorism financing usually raised in connection with the anonymity of the use of virtual currencies," he says.

Other proposed amendments to AMLD4 put forward by the EC include measures requiring countries to harmonise their enhanced due diligence rules for high-

risk nations. Member States would be obliged to transpose new provisions into their national laws, affecting virtual currency exchanges, e-wallet providers, banks and other 'obliged entities'. According to Mr Taylor, the amendments would also require digital platforms to apply Customer Due Diligence (CDD) when exchanging virtual to real currencies and to report suspicious activity to government entities. "Recent developments suggest increased regulatory scrutiny and future obligations for virtual and crypto currencies may become even more far-reaching," he says. However, the central register element has become a lightning rod for criticism, and operational challenges will materialise since the Directive removes automatic Simplified Due Diligence (SDD) entitlement.

Challenges for compliance

Once individual Member States work the Directive into their national laws, companies will face tough new compliance obligations, particularly those operating in the cryptocurrency space. AMLD4 provides for financial penalties, criminal prosecution and potential imprisonment for non-compliance. Accordingly, compliance professionals will be required to review and update their policies and procedures. This includes risk assessments, rigorous customer due diligence and on-boarding practices. Companies must take a more focused approach to their business partner and customer due diligence controls, enhancing measures for higher risk countries, sectors, entities, products and individuals. If firms treat compliance as a tick-box exercise, or choose to ignore compliance requirements, there will be penalties.

Another key area of review is politically exposed persons (PEPs). Under AMLD4, the definition of PEPs has been extended to include citizens holding prominent positions in their home country, such as politicians, the judiciary and senior members of the armed services, as well as those of overseas countries. Furthermore, the Directive has moved to clarify the status of family members of PEPs, noting that parents, spouses (or equivalent partners), children and their spouses or partners, are now to be treated as PEPs.

"The removal of automatic application of SDD, expanded PEP definition and increased CDD requirements for PEPs are some of the changes required by AMLD4 which may require compliance professionals to revisit their customer risk classification criteria and understand the downstream operational effects of such changes," says Mr Taylor. "This may include due diligence requirements, transaction monitoring and screening, among others. Adoption and interpretation of the AMLD4 requirements into existing policies and procedures, culture, controls and systems to maintain an effective AML programme will be the key challenge facing compliance professionals."

Compliance professionals will certainly have their hands full under the new Directive. "The compliance

professionals of obliged entities will have to carefully review their internal standards and procedures as to their compliance with the new requirements," says Dr Kunz. "To that end, a gap analysis will be crucial. For virtual currency platforms, the adjustment to the new AML-framework will, for obvious reasons, be more challenging than for companies which are already 'obliged entities'."

AMLD4, like other regulatory and legislative developments in the AML and FTC space worldwide, is a welcome and much needed measure. Of course, companies operating in AMLD4-compliant countries will have new and taxing considerations to make. But failure to adhere to the new requirements could have financial and reputational repercussions, as the fight against financial malfeasance goes on. R&C

EXPERT FORUM

FCPA, AML AND OFAC RISKS FOR PRIVATE EQUITY AND HEDGE FUNDS

PANEL EXPERTS

Harvey Kelly
Managing Director
AlixPartners
T: +1 (646) 746 2422
E: hkelly@alixpartners.com

Harvey Kelly is managing director and global financial advisory services leader at AlixPartners. He has over 30 years of experience as a financial consultant specialising in forensic reviews, litigation consulting and auditing. A former partner with PricewaterhouseCoopers LLP, Mr Kelly has represented boards of directors, investors, creditors and federal courts in financial investigations. He has led investigations in over 30 countries. He has performed such services in connection with internal reviews, legal proceedings and regulatory investigations. Mr Kelly is often called upon to serve as an independent examiner or similar post-event monitoring role as required by settlement and deferred prosecution agreements between organisations and their regulators.

James Walker
Partner
Richards Kibbe & Orbe LLP
T: +1 (212) 530 1817
E: jwalker@rkollp.com

James Walker is a partner in Richards Kibbe & Orbe LLP's New York office. He concentrates on internal investigations, civil litigation and professional liability. Mr Walker regularly represents audit committees, directors, senior executives and other professionals in government and internal investigations of potential criminal, regulatory and/or professional misconduct, and in related civil litigation.

Rolf Lindsay
Partner
Walkers
T: +1 (345) 914 6307
E: rolf.lindsay@walkersglobal.com

Rolf Lindsay joined Walkers in 2005 and is a partner in the firm's Global Investment Funds Group. His practice focuses primarily on private equity funds and their activities, and encompasses the structuring of fund sponsor vehicles, the formation of alternative investment funds and the consummation of transactions undertaken by them.

Mark Schein
Chief Compliance Officer
York Capital Management LP
T: +1 (212) 300 1372
E: mschein@yorkcapital.com

Mark David Schein, J.D. is the chief compliance officer and managing director at York Capital Management. Mr Schein joined York Capital Management in 2005. He spent three years at US Trust Company and Schwab Capital Markets, where he served as director of broker-dealer compliance and director of anti-money laundering, respectively. He served as the chief compliance officer of York Enhanced Strategies Fund, LLC. Mr Schein worked for six years as an assistant district attorney in Bronx County and five years as a trial counsel in the New York Stock Exchange's Enforcement Division.

RC: Could you provide an overview of the current scrutiny private equity and hedge funds are under in connection with FCPA, AML and OFAC regulations? Are fund managers now spending more time and resources on reducing risks and exposures in these areas?

Kelly: FCPA and OFAC regulations apply to entities conducting business in or through US means. Anti-money laundering (AML) rules and regulations are promulgated under Section III of the USA PATRIOT Act. With the passage of Dodd-Frank, many hedge funds are required to register as registered investment advisers (RIAs) under the Investment Advisors Act of 1940. Though there is no clear regulatory requirement to do so, RIAs are covered under the criminal provisions of the Money Laundering Control Act. Today, many RIAs have developed internal policies and procedures to address exposure to AML, FCPA and OFAC due to tightened scrutiny into transactions by financial institutions.

Walker: In 2016, the US Justice Department increased the size of its FCPA unit by 50 percent and announced a pilot programme that provides guidance for corporate resolutions of FCPA investigations that strongly encourages self-disclosure, cooperation, and remediation (where appropriate). The pilot programme demonstrates the government's commitment to FCPA enforcement and has motivated private equity and hedge funds to enhance their anticorruption compliance programmes. Funds also have a clear directive to implement comprehensive internal controls to achieve AML and OFAC compliance in the wake of FinCEN's 2015 announcement of a proposed rule that will bring SEC registered investment advisers under the Bank Secrecy Act and USA PATRIOT Act for purposes of AML compliance. RIAs will be required to implement a comprehensive written compliance programme designed to prevent money laundering and terrorist financing.

Lindsay: Although the FCPA is US legislation, the take away from an offshore perspective is that the FCPA has a broad extraterritorial reach. The Cayman Islands has its own anticorruption legislation, which sets out extensive local and international corruption offences. Practically speaking, managers of funds could potentially face liability for FCPA breaches and breaches under the Cayman Islands equivalent legislation. OFAC enforces the US sanctions regime, which has a similarly wide extraterritorial reach. Investment funds navigating the global marketplace must tread carefully as sanctions can cover a variety of targets, apply to offshore affiliates and can change frequently. As a British overseas territory, the Cayman Islands implement the international sanctions obligations of the UK in

addition to its own autonomous terrorist sanctions regime. For funds domiciled in the Cayman Islands, AML scrutiny is nothing new. Funds are subject to a Cayman Islands AML regime, which is equal to or exceeds accepted global standards. This includes an obligation to have in place policies and procedures to address AML obligations, which may, and often are, typically delegated to professional third-party administrators. Funds that carry out AML requirements internally are required to satisfy the Cayman Islands AML regime by, among other things, adopting an appropriate AML manual, appointing a person internally to be responsible for AML compliance and having procedures in place for constant monitoring.

Schein: FCPA, AML and OFAC are currently areas of severe scrutiny for hedge fund and PE managers, and for good reason. As private investments and deals with counterparties and joint ventures become a larger part of the investment landscape, there are more opportunities for funds to run afoul of the rules. Most likely, a firm could hire a consultant or representative who does something improper and the firm is ultimately held responsible for those actions. The result of this is that firms are now spending much more time and resources on ensuring that their employees are trained to recognise hazardous situations. Compliance and legal teams are spending more time monitoring their firm's dealings with an eye toward preventing any AML or FCPA violations.

> **"Although the FCPA is US legislation, the take away from an offshore perspective is that the FCPA has a broad extraterritorial reach."**
>
> *Rolf Lindsay, Walkers*

RC: How would you characterise government compliance and enforcement actions against PE and hedge funds? Has there been an uptick in investigations?

Lindsay: From an offshore perspective, we have seen more investigations and auditing of fund managers, which predominantly do not result in enforcement actions against PE and the hedge funds themselves. The level of government compliance and enforcement depends very much on where the fund manager is based. In Dubai, the Dubai International Financial Services Authority (DFSA) is very hands

on and carries out regular audits of DFSA regulated managers to ensure they are in compliance. In Hong Kong, the Hong Kong Securities and Futures Commission (SFC) applies a similarly stringent standard of regulation on managers of offshore funds. More recently, the SFC has taken a more robust approach in its inspection and enforcement actions, and the Inland Revenue Department has increasingly been looking at the tax treatment of PE funds.

Schein: There has been an uptick in investigations. Presently, the regulators and prosecutors' offices have increased their focus on FCPA issues. This comes at a time that as a result of economic and market circumstances, private and joint venture deals are more attractive to firms. The result is that there is a perfect storm of increased scrutiny at a time when there is much more to scrutinise.

Walker: Media reports have identified government investigations focused on two areas of investing activity by private equity firms: corruption risk arising from investments involving sovereign wealth funds, pension funds or other government funding, and funds investing in portfolio companies that operate in jurisdictions and industries where the corruption risk is high. With respect to portfolio company investments, the 'Resource Guide to the US Foreign Corrupt Practices Act' identifies the degree of a company's ownership and control over portfolio companies as a factor that will impact a private equity firm's potential FCPA exposure. Firms would be remiss, however, to think that partial ownership – even less than majority ownership – of a portfolio company will dissuade government investigators from looking to them for liability when corrupt payments have been uncovered, particularly where there are other significant indicia of control by the fund and the fund has not implemented adequate internal controls.

> **"It is important that fund managers prioritise customer and counterparty due diligence and risk management."**
>
> *Harvey Kelly, AlixPartners*

Kelly: Over the past few years we have seen alternative investment vehicles, including hedge funds, face enforcement actions and related criminal or civil charges related to the FCPA, for example. A key area of focus for regulators has been the

dealings these funds have had with sovereign wealth funds, some of which have led to investigations. In 2002, the Financial Crimes Enforcement Network of the US Department of Treasury (FinCEN) began to clarify AML obligations for investment companies and private equity funds. In 2015, FinCEN proposed new rules that would extend AML requirements to federally registered investment advisers. The rule would raise compliance expectations, even for those RIAs that already have AML programmes in place by mandating internal controls and independent testing.

RC: What, in your opinion, are the most critical compliance issues currently facing fund managers? What steps are they taking in response to increasing regulatory expectations?

Walker: Ensuring the security of client funds, identifying conflicts of interest and conducting appropriate due diligence are critical to FCPA, AML and OFAC compliance. Investor funds are jeopardised whenever a fund manager fails to identify and address potential conflicts in a proposed investment, or to appropriately assess corruption risk. Fund managers are realising that they must look beyond straightforward legal prohibitions – for example, prohibited transactions with Specially Designated Nationals (SDNs) – and conduct a more meaningful risk assessment that adequately contemplates the 'association risk' of transacting with counterparties and intermediaries who have been connected to corrupt transactions.

Kelly: It is important that fund managers prioritise customer and counterparty due diligence and risk management. Given the financial penalties and reputational risk that can come with an enforcement action, fund managers should consider counterparties and customers within the context of their potential risk. Under OFAC rules and regulations, fund managers are prohibited from conducting business with certain SDNs or entities and jurisdictions. But the specific steps a fund should consider depend on the risks it faces – meaning, regions in which a fund operates or which entities it does business with. Essentially, it is important to develop appropriate risk management practices to establish a system of internal controls and systems that can help to prevent potential OFAC violations.

Schein: Compliance departments are faced with several challenges on the AML/FCPA front. First and foremost among which is keeping track of what deals and what activities their firms actually participate in. These deals tend to be global and an investment person can get involved in a deal somewhere around the globe and not inform his compliance staff of what he is doing. He can partner with an unsavoury person or entity, or do a deal in a prohibited jurisdiction – all without checking with compliance back at headquarters. Often, the investor

does not even realise he is putting his firm at risk. It is paramount that the compliance team has a process of oversight and review which allows it to monitor the investment staff's activities. Frequent training is also important in order to ensure that investment staff are fully aware of the risks and pick up the phone or send an email to inform compliance. It is also crucial that compliance stays informed about the laws and regulations in different jurisdictions so that the firm does not inadvertently cause a violation.

Lindsay: Compliance with Know Your Client (KYC) rules, AML and sanctions screening is one of the most critical issues facing fund managers today. Fund managers are required to perform and document detailed due diligence on investors and failure to do so can have severe consequences. Following the implementation of US and UK FATCA, and, more recently, the 'common reporting standard', investors must now also be checked for tax residency. We see fund managers investing more in technology and compliance personnel to meet the volume and diversity of regulatory demands and reporting requirements.

RC: What advice can you offer to fund managers on how to avoid FCPA, AML and OFAC violations, avoid sanctions risks and, ultimately, strengthen their compliance programmes? What are the essential elements of a 'culture of compliance'?

Schein: Training and frequent interaction with the investment staff is key to a strong compliance programme. A good compliance officer must get up from their desk and interact with investment staff wherever they are. It is impossible to properly tailor a compliance programme if you are unsure of what exactly your employees are doing all across the globe. If these complex investment deals were easily understood and anticipated by compliance officers, we would not be compliance officers. Therefore, it is important to visit investment staff and discuss, in detail, the deals that they are proposing and who they are hiring to help them facilitate the transactions. In addition, if the investment personnel are not familiar and comfortable with the compliance staff there is little chance they will remember to reach out to us while working on a project. If you visit with them, ask questions and answer questions, you will be thought of as an ally and a sounding board to help with the transaction. Lastly, there is no culture of compliance without strong support from senior management. Invariably, there will be times when the business side wants to complete a deal and compliance needs to slow things down or actually prohibit the transaction. These situations will be escalated to senior management and it is crucial that senior management takes the conservative approach and sides with compliance. I have been lucky enough to see first-hand how that type of support cultivates a culture within a firm where people make

the conservative decision and protect the franchise before taking a risky approach.

Lindsay: A fund manager needs to understand its legal requirements and design a robust compliance programme to deal with each of the separate areas of regulatory focus. While there is no 'one size fits all' compliance programme, fund managers should tailor their compliance programmes based on the legal requirement and an accurate assessment of applicable risks – for example, the investor base, the jurisdictions in which the fund operates, the nature and extent of its interactions with foreign government entities and the use of placement agents and other third party intermediaries. It is not simply enough to have written compliance programmes in place, there must also be a 'culture of compliance' within a fund manager to ensure that it is not just the members of the compliance team carrying the burden.

Kelly: It is important for fund managers to establish a system of internal controls to FCPA, AML and OFAC rules and regulations. A system of internal controls should include compliance policies, procedures, the designation of a compliance officer, an independent audit function and employee training. Also, funds should seek to establish a culture of compliance – one that can ensure that policies and procedures are viewed as being as important as the fund's business objectives. When considering the level of enforcement action they will take, regulators usually look at an institution's culture of compliance, and the actions taken by groups such as senior management and boards of directors.

Walker: Fund managers need to create a 'culture of compliance' that effectively avoids sanctions risks. This requires leadership by senior management to implement a programme of credible and defensible pre-acquisition anticorruption due diligence and post-acquisition monitoring and auditing. Fund managers must ensure that risk-based due diligence addresses FCPA, AML and OFAC risks through a genuinely holistic approach, with a longer term view of how entering into any transaction without adequately assessing the risk can significantly harm investors and the fund. Senior management must consistently demonstrate the importance of ethical business practices to an employee's success in the company, and communicate with investment staff about deals that were rejected because the corruption risk was deemed too high.

RC: What are some of the potential consequences for fund managers that fail to establish an adequate level of controls or carry out due diligence when screening investors, third-party providers and others?

Kelly: Violations of FCPA, AML and OFAC rules and regulations can lead to both civil and criminal fines,

reputational harm and even shareholder litigation. To establish an adequate level of control, an initial step would be to conduct a risk assessment that addresses the various requirements under FCPA, AML and OFAC regulations. This exercise should involve multiple parts of the business and include board members, senior management, compliance, audit and people in the business. The goal should be to assess the current risks that business activities, customers and counterparties pose and to create a system of internal controls. It is important that funds fully understand the nature of customer and counterparty relationships and potential risk exposure.

Walker: Failing to establish adequate controls may, at a minimum, cause reputational damage and investor unrest when the press links the fund with disreputable co-investors and third parties, but is increasingly more likely to result in serious civil and criminal penalties – including disgorgement, substantial money penalties and possibly criminal conviction of the corporate entity and individuals – if the government discovers corrupt payments, money-laundering or funnelling of funds to terrorist organisations. Indeed, a fund's failure to properly assess risk and respond to red flags could cause a fund to close its doors if investors representing substantial assets-under-management flee on the heels of the government's announcement of the underlying misconduct. Further, the investigation findings and resolution with the government may trigger breaches of contractual covenants, exposing the fund to an inability to meet its financial obligations and civil lawsuits by counterparties and investors, who will also sue to recoup financial losses.

"Senior management must consistently demonstrate the importance of ethical business practices to an employee's success in the company."

James Walker,
Richards Kibbe & Orbe LLP

Lindsay: Non-compliance is a serious matter and managers can face significant fines, other penalties as well as imprisonment. Under the Cayman AML Regime, failing to report knowledge or suspicion of money laundering and failing to have suitable procedures in place for client or customer identification, record keeping and internal control and communication, are criminal offences. Under the Cayman Islands regime, penalties for breaching sanctions can vary however, in general terms, any

individual found guilty of an offence is typically liable on conviction to imprisonment we well as a fine.

Schein: If a firm fails to establish the adequate level of controls, or cuts corners, the results will be catastrophic. Clearly, it can result in violating AML laws or doing business in sanctioned nations. But an inadequate process of screening investors and transactions can also lead to fraud in which investors lose money, personal information is hacked, civil litigation ensues and the firm is at risk.

RC: For fund managers looking to invest in businesses in Cuba, Russia or Iran, what steps should be taken to mitigate the risk of violating sanctions restrictions against these jurisdictions?

Lindsay: Active compliance with a sanctions programme is imperative. Fund managers who are looking to invest in these jurisdictions need to identify the exact provisions of the corresponding sanctions order, which are generally very prescriptive. Sanctions are subject to frequent change, so must be closely monitored on an ongoing basis. The Cayman Islands maintains a published list of sanctions orders that have been given effect in the Cayman Islands. Currently, by way of example, there are no Cayman sanctions in force in Cayman against Cuba, but the position is different for the US.

Schein: The compliance and legal departments should be brought into transactions early enough to provide guidance to the business units. The regulatory side of the business should have an understanding of what transactions the business units are proposing and review those transactions, not just internally, but also with outside counsel who specialise in sanctions compliance. A thorough process will go a long way towards allowing the business units to focus on their deals without the risk to the firm.

> **"If a firm fails to establish the adequate level of controls, or cuts corners, the results will be catastrophic."**
>
> *Mark Schein, York Capital Management LP*

Walker: Economic sanctions against Russia arising from political moves involving Ukraine and Crimea, a lifting of significant sanctions but

maintenance of others against Iran, and the US trade embargo on Cuba – even in the face of eliminating certain travel, telecommunications and agriculture restrictions – means that opportunities for most funds to do business in those jurisdictions remain limited or are years away. The first step for funds contemplating business in Cuba, Russia or Iran is establishing a comprehensive compliance programme characterised by thorough anticorruption and anti-money laundering procedures, seamless collaboration between compliance personnel and investment professionals, effective auditing and monitoring, and a comprehensive database reflecting diligence on past and contemplated counterparties, third parties and intermediaries, with regular updating and cross-checking. Funds then will need to work closely with outside experts to understand how pertinent restrictions affect the fund's business plans, and be ready to respond timely to the ever-changing regulatory landscape.

Kelly: It is important that fund managers recognise that Cuban, Russian and Iranian sanction regimes are distinctly different both in both their scope and reach. Russian sanctions target certain businesses and individuals, as well as certain types of transactions. Cuban and Iranian sanction regimes are broader and, in the case of Cuba in particular, continue to evolve. It is important for fund managers looking to invest in these countries to conduct enhanced due diligence on customers, counterparties and investments. Also, managers should determine whether a particular investment is permissible under a general licence issued by OFAC, if a special licence should be sought from OFAC, or if the investment may be prohibited.

RC: Do you expect the risks arising from FCPA, AML and OFAC will increase in the months and years to come? Do fund managers need to do more to prepare themselves against regulatory actions?

Walker: Risk to private equity and hedge funds arising from FCPA, AML and OFAC will only increase as regulators continue to hold companies and individuals accountable for corrupt practices. Funds can no longer merely tout implementation of risk-based anticorruption compliance measures that heighten scrutiny of transactions in high risk jurisdictions or involving high risk counterparties. Instead, in addition to heightened policies and procedures, funds need to incorporate into their risk assessment the potentially devastating effect if their training, diligence, testing, auditing and monitoring are insufficient to identify and avoid corruption.

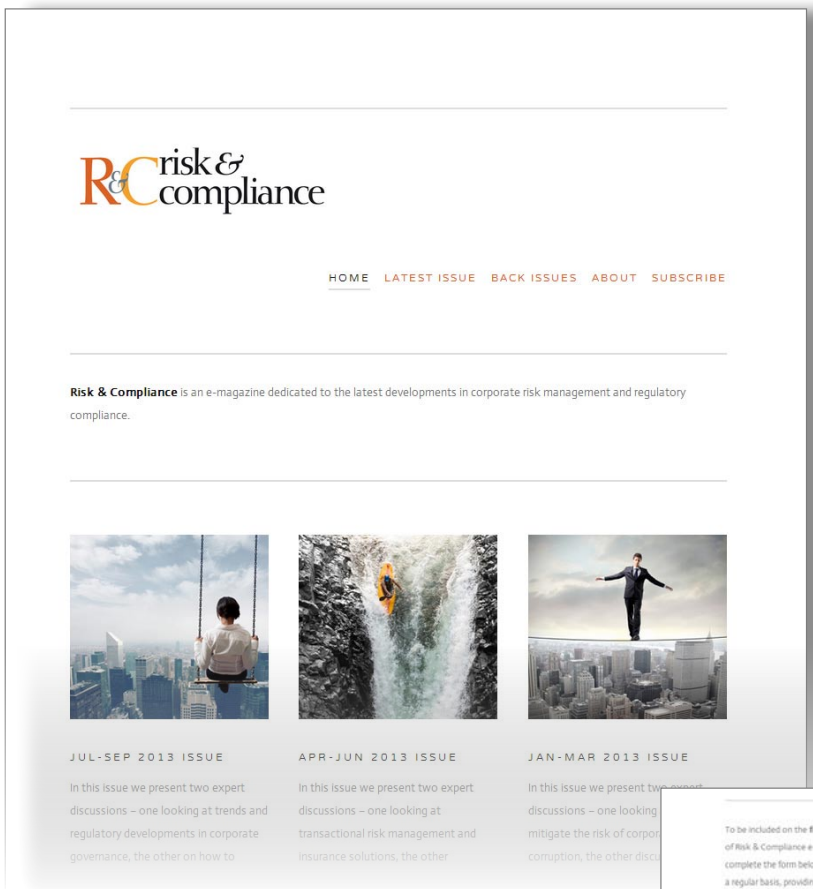
Kelly: The continued growth of the industry, particularly with investments overseas, means it will remain important for fund managers to focus on FCPA, AML and OFAC risks. One approach for fund managers would be to measure their compliance efforts with those of peers and the broader financial

services industry. Although there is currently no codified requirement for fund managers to monitor customer or counterparty activity, for example, this is an area that should be looked at in terms of the risks these areas may represent for managers.

Schein: The risks will continue to grow because the laws and rules will continue to expand and become more complex. Fund managers need to continue to prioritise compliance with the laws even at the expense of forgoing deals which could be profitable but carry a high level of risk.

Lindsay: There is no sign that regulation across these areas is abating. With ever increasing cooperation among global regulators and enforcement agencies, bribery and corruption investigations that start in one part of the world can often spread to another. It remains to be seen whether increased global cooperation will translate to more standardised reporting templates which would help ease the burden on managers. R&C

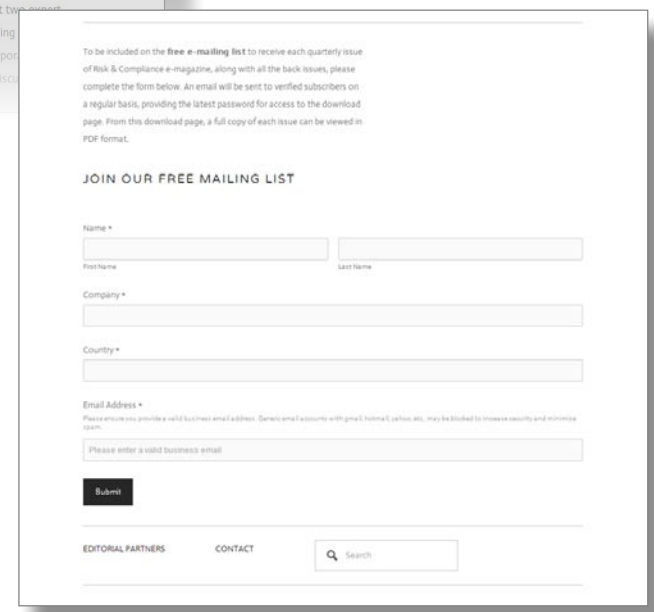
www.riskandcompliancemagazine.com



1. Visit the new website

2. Sign–up to our free emailing list

3. Forward the link to colleagues and clients



4. Receive and enjoy future copies of Risk & Compliance

PERSPECTIVES

BRIBERY AND CORRUPTION IN THE UAE – MANAGING BRIBERY INVESTIGATIONS

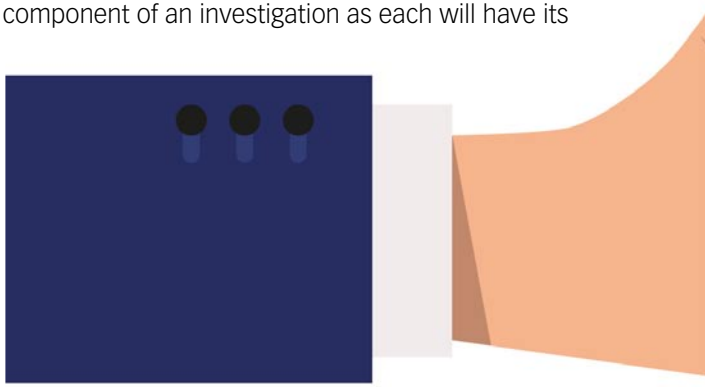
BY **JUSTIN MCCLELLAND, FADIL M. BAYYARI AND BIBI SARRAF-YAZDI**
> WINSTON & STRAWN

In recent years, a number of international surveys and reports have benchmarked countries on the basis of their perceived levels of corruption. The UAE's position, 23rd lowest of 168 countries, suggests that combating bribery and corruption are key areas on which organisations should focus.

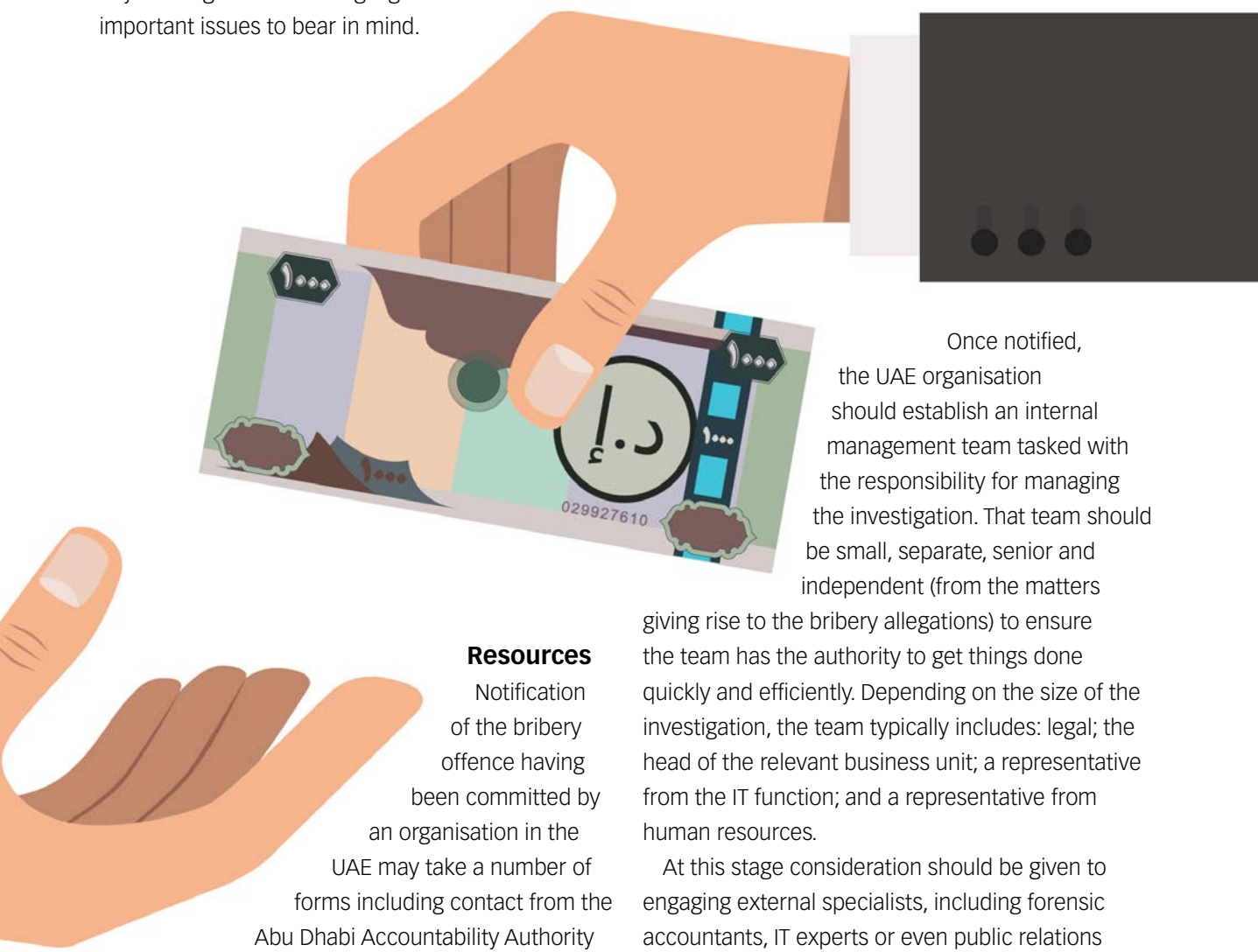
Globally, increased perceived levels of bribery and corruption, coupled with emboldened prosecuting agencies using established (e.g., the US's Foreign and Corrupt Practices Act 1977) and newer (the UK's Bribery Act 2010) legislation have raised the importance of being properly prepared. In the UAE, enforcement of its established anti-corruption laws has received a boost with the Abu Dhabi Executive Council announcing the establishment of a new Anti-Corruption Unit in May 2015.

The investigation process

It is not possible to map out every individual component of an investigation as each will have its



own features depending on the nature, scope and jurisdictional spread of the alleged behaviour. However, it is possible to identify the key phases for any investigation and to highlight some of the important issues to bear in mind.



Resources

Notification of the bribery offence having been committed by an organisation in the UAE may take a number of forms including contact from the Abu Dhabi Accountability Authority (ADAA) and/or the Ministry of Justice (MOJ), or from an internal process, e.g., internal whistleblowing, internal audit work or routine accounting checks.

Once notified, the UAE organisation should establish an internal management team tasked with the responsibility for managing the investigation. That team should be small, separate, senior and independent (from the matters giving rise to the bribery allegations) to ensure the team has the authority to get things done quickly and efficiently. Depending on the size of the investigation, the team typically includes: legal; the head of the relevant business unit; a representative from the IT function; and a representative from human resources.

At this stage consideration should be given to engaging external specialists, including forensic accountants, IT experts or even public relations

teams (if necessary, in multiple jurisdictions). Complex factual investigations and legal analysis may need to be conducted quickly, making it likely that the organisation will engage external legal advisers.

The internal team and external advisers will need to focus on obtaining answers to the following pivotal questions: (i) identifying what appears to have happened and when, and who was involved; (ii) whether the behaviour is continuing (and, if so, how to stop it); (iii) whether there is any foundation to the allegations; (iv) who is affected by the allegations (both internally and externally); (v) the risks to the organisation; (vi) the jurisdictions affected by the bribery; and (vii) how the organisation can communicate its position at an appropriate time (both internally and externally).

As the investigation evolves, these issues should be reviewed to ensure that the investigation remains properly focused.

The internal investigation

At the first meeting of the management team, an internal team should be set up to investigate the alleged behaviour. This team will develop an investigation plan, building in flexibility to accommodate challenges to resources and timings as the work progresses. The key tasks and issues for the investigative team, which should be included in the plan, are outlined below.

Gathering and securing evidence. Preserving all relevant or potentially relevant evidence relating to the alleged behaviour will be crucial, and is likely to be requested by the ADAA and/or the MOJ. Any gaps in evidence, either because the data was lost or destroyed, may impede the organisation's own ability to understand what happened and could cause significant problems in subsequent associated litigation, or in further investigations by the regulators or prosecuting agencies.

> **"Preserving all relevant or potentially relevant evidence relating to the alleged behaviour will be crucial."**

Data review. The management of the review process can be assisted using document management platforms to allow a proportionate, targeted and prioritised review.

Interviews. Conducting interviews with relevant (both current and ex) employees and (possibly)

external third parties should be planned. The timing of interviews should be considered carefully as, where the internal investigation is being conducted in parallel with investigations by regulators or prosecuting agencies, those regulators or agencies may object to certain witnesses being interviewed in the course of an internal investigation. Interviews should be conducted by experienced interviewers and accurately recorded in a note, with the privileged status of that note made clear.

Employees. A challenging issue in any investigation is whether, and at what stage, to suspend employees who may have engaged in bribery or corruption. Much will depend on the information available when the management team makes this decision and whether a suspension (or suspensions) would be deemed compliant with the disciplinary rules of the UAE Labor Law, Federal Law No. 8 of 1980, as amended.

Written report. It may be appropriate for the investigative team to prepare a written report which would typically include: a description of the nature and extent of the internal investigation; an overview of the factual findings; the conclusions reached; and the steps taken as a result of the factual findings together with a list of future intended actions. However, a report is not without risks and care should be taken in reaching any conclusions regarding any criminal or regulatory infringements.

The Regulators and prosecuting agencies

It will be important from the outset of an investigation to set a cooperative but firm tone with the ADAA, the MOJ and other regulators or prosecuting agencies. Where the behaviour under investigation extends across more than one jurisdiction, the management team will need to take into account the possibility of having to self-report the behaviour, which raises a number of challenging issues.

As to the final outcome, there may be scope to persuade regulators or prosecuting agencies that insufficient evidence or public interest exists to justify action, or that early cooperation justifies a less aggressive regulatory response or a mitigated penalty. However, the organisation must not lose sight of the fact that any settlement which involves the admission by an organisation of criminal behaviour will very likely affect its position in civil proceedings and under its insurance policies.

Associated litigation

Litigation associated with the (alleged or admitted) bribery and corruption may come from a number of potential sources and arise across different jurisdictions. To address associated litigation risks, the management team should formulate an initial defence strategy early in the investigation following an initial internal audit of the immediately available evidence. This enables the organisation to take a

preliminary view on whether there is any evidential or legal foundation for potential allegations or for the matters being investigated. The strategy should take into account preservation and gathering of documents relevant for the defence of any litigation and preserve privilege in the documents from disclosure in any litigation.

Conclusion

With the increased likelihood of bribery and corruption allegations arising, having a plan to manage the myriad issues that they generate from initial emergence of the allegation will help UAE organisations in addressing these challenges efficiently and effectively.

The authors would like to thank Robb Adkins and Derek Andreson, partners at Winston & Strawn, for their contribution to this article. R&C

Justin McClelland
Partner
Winston & Strawn
T: +44 (0)20 7011 8736
E: jmcclelland@winston.com

Fadil M. Bayyari
Associate
Winston & Strawn
T: +971 4 424 2332
E: fbayyari@winston.com

Bibi Sarraf-Yazdi
Associate
Winston & Strawn
T: +44 (0)20 7011 8767
E: bsarrafyazdi@winston.com

ONE-ON-ONE INTERVIEW

MANAGING THIRD PARTY AND COUNTERPARTY RELATIONSHIP RISKS

Bob Conlin
President & CEO
NAVEX Global
T: +1 (866) 297 0224
E: insight@navexglobal.com

As president and CEO of NAVEX Global, Bob Conlin leads the executive team and serves as a member of the board of directors. He leverages more than 25 years of senior management experience in operations, sales, marketing, product management and business development to champion NAVEX Global's vision, strategy and execution. Before joining NAVEX Global, Mr Conlin served as senior vice president of marketing and business development at Accero, a global provider of human capital management solutions. In 2016, he was named 'Technology Executive of the Year' by the Technology Association of Oregon.

RC: Could you outline some of the major risks that can emerge from third party and counterparty relationships in today's business world? What red flags should firms try to identify?

Conlin: In our most recent 'Ethics & Compliance Third Party Risk Management Benchmark Report', bribery and corruption by third parties was the top concern among survey respondents at 39 percent. Fraud, at 23 percent, conflicts of interest at 19 percent, and safety & occupational hazards at 10 percent rounded out the top four. With these concerns in mind, there are some red flags to watch out for. First, a lack of cooperation or unwillingness to cooperate in the due diligence process, or inability to produce necessary and expected documentation. Second, clear ties to foreign government officials. Also watch out for a lack of evidence of relatable qualifications for the particular job or service the third party is expected to provide. Other key red-flag indicators include previous documented failures, indictments or negative press about the third parties; compensation that does not relate to standard rates or payment patterns — such as success fees, cash payments or payments to offshore accounts — and lack of a standard, pre-engagement written agreement. Also of concern is if the organisation displays an unwillingness to certify its third-parties' policies or grant auditing or monitoring rights. Another indicator is general or unclear explanations behind payments made by the third party. Finally, be wary of generally poor documentation and record keeping. It is critical to evaluate these red flags before and throughout your business relationships with third parties.

RC: What particular risks can emerge in relation to a company's supply chain? How can supply chain delays be minimised and supplier compliance maintained?

Conlin: It is easy for organisations to become overly dependent on one or two third parties. If an unexamined or unmonitored strategic partner has a compliance or supply chain failure, they may no longer be a suitable source of goods or services. As a result, the organisation will have to scramble to replace that third party. This will create critical shortages that could disrupt the organisation's supply chain, reputation and bottom line. To minimise delays in selecting new third parties, it is smart to conduct early due diligence on the top candidates who may be responding to a request for proposal (RFP). This eliminates the instance in which the procurement team spends significant time and energy selecting a top candidate and then puts them through due diligence only to find that there is a red flag that disqualifies them. In addition to delays, this may cause the organisation to lose bargaining power.

We recommend that pre-engagement due diligence be conducted on the top-tier candidates before deciding. Additionally, our third-party benchmark survey found that organisations rate their own third-party programmes more positively when they use outsourced third-party automation systems – a finding affirmed by what we see in our day-to-day interactions with customers. Organisations should automate every part of the due diligence process they can. It will improve quality and speed and provide the ability to document and track compliance steps, such as policy certification, monitoring and auditing. Our recent benchmark report noted an additional benefit from automation: reduction in legal actions and fines.

RC: Is there any advice you can give to firms on implementing and maintaining robust monitoring systems? To what extent can this be customised for the type of third parties they will be dealing with?

Conlin: Ongoing monitoring is critical, and often overlooked after a third party is engaged. Difficulty monitoring third-party relationships is the issue that respondents to our survey said most undermines their programmes' effectiveness. In addition to adding elements to the organisation's annual internal audit plan, there should be "some form of ongoing monitoring of third party relationships", according to 2012 Guidance from the Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) regarding the Foreign Corrupt Practices Act (FCPA). Many of the top monitoring concerns could be addressed through automated due diligence software. Automation allows organisations to demonstrate a defensible process designed to ensure that no new risk has arisen since the initial due diligence and, if something has arisen, the organisation has quickly dealt with it. If the risk warrants mitigation, a 'freeze' on the relationship, termination of the third party, an internal investigation, and possibly self-disclosure to regulators all build credibility with regulators. When it comes to customising a monitoring programme, regulators, and guidance on effective third-party

"Organisations should automate every part of the due diligence process they can."

Bob Conlin, NAVEX Global

compliance programmes, recognise that the best approach is risk-based. A reasonable process, including a determination and response to the risk each vendor poses to the organisation, is all that is required. If this is consistently applied, due diligence and monitoring can be adjusted accordingly.

RC: With regard to processes and systems, should firms avoid taking the word of their third-party partners at face value? What steps should they take to verify the adequacy of their partners' systems and processes?

Conlin: Every organisation has longstanding relationships with suppliers, vendors, third parties and other consultants. These relationships, when they are positive, create a currency of good will and trust. However, in today's world simply 'taking their word for it' is a dangerous approach. The right questions need to be asked and appropriate followups should occur based on the responses and other risk factors. Scrupulous third parties should not object to what has now become best practice – due diligence, documentation and monitoring. Obviously, if the third party is going to have access to, or possession of, sensitive information – such as client lists, personally identifiable information, proprietary information, and so on – the risk is even greater and more due diligence and stress-testing is appropriate. Also, there are internal control certifications that may be requested from clients or the organisation's other partners and these have to be honoured. With respect to systems and processes, involve SMEs, audit, cyber security experts and definitely the organisation's IT department. There are many other factors to consider, including past experience with the third parties, the third party's geographic location, local laws, client contract requirements and the technical and technological sophistication of the third party. Risks occur regardless of the intent of the third party; a well-meaning third party may still cause havoc. Recent examples of this include a situation where a third party's weak software was used as the gateway by a hacker to access and infiltrate an organisation's databases. In addition to stress testing the processes and systems, all third party employees should receive training on the written policies of an organisation with respect to the use of IT systems, identifying spam and phishing emails, downloading unapproved software and proper use of mobile devices.

RC: What are some notable failures in managing third party and counterparty relationship risks? In your opinion, what went wrong in those circumstances and what can firms do to ensure they do not end up in a similar situation?

Conlin: Bribery and corruption was the top concern of industry professionals in our last third-

party benchmark report. A significant number of recent bribery and corruption cases in the US and around the world involve compliance failures by a third party acting on behalf of an organisation. This includes third parties offering bribes to foreign government officials or government instrumentalities to win or retain contracts, increase the use of the organisation's products or to obtain favourable tax treatments. There are steps that organisations can use to reduce a similar risk. First, ensure the organisation has a culture of compliance with all laws and align this culture with internal controls and compliance programme goals and resources. Second, conduct risk-based due diligence on prospective third parties and continuously monitor them via automation. Third, follow and document the third-party policy and process. Fourth, have a clear policy on the use and acceptable practices of third parties on behalf of the organisation. Fifth, communicate this policy to third parties and require certification and audit adherence. Finally, require third parties to demonstrate their compliance programmes and training.

RC: What steps can firms take to overcome legal and cultural barriers to the monitoring process when working with third parties in emerging markets?

Conlin: It is a good idea to work with experienced third parties who have partnered with other organisations based in countries with compliance histories and expectations, and to look for good culture matches. These may be found by looking at third parties' codes of conduct, anti-bribery and corruption policies, and training records. At the same time, organisations should share their own policies with third parties and explain the 'why' when it comes to their rationale. It should be made clear that no individual third party or country is being singled out – that everything is process-driven and risk-based. This is especially important in emerging markets. Organisations entering such a market may want to do so incrementally. For example, do not give all of an organisation's business to a single, untested third party if at all possible. Start small and see how the third party reacts to monitoring. Then, consider increasing the scope of work for those that are compliant. Another way to reduce the cultural barriers is to use proven third parties, especially those with ties to other organisations based in developed countries or where the third party itself is multinational. These organisations will be much more familiar with the best practice expectations surrounding monitoring. Lastly, regularly reach out to third parties; get and give feedback. Where appropriate, show the third parties that you are listening to their feedback and concerns, even if you cannot, or will not, adopt or accept it.

RC: How are regulatory and legislative changes influencing the way

companies deal with third parties and counterparties? Do you foresee any regulatory or legislative change in the near future?

Conlin: While the publicity associated with third-party compliance failures and the accompanying penalties is accelerating regulation changes, regulators and organisations are still trying to find a balance between oversight and the ability to conduct business across borders. In recent years, new standards have been rolled out regarding these issues, such as ISO 19600 in 2014. Many cases involving third parties stem from bribery and corruption. We are seeing a greater focus from the DOJ regarding individual accountability in this area – the September 2015 Yates memo, for example. As well, the DOJ and the SEC have both added additional investigative resources and are getting more global cooperation, leading to additional international laws being created. Lastly, in late 2015, the DOJ hired banking industry compliance executive Hui Chen as its compliance counsel to help review the effectiveness of compliance programmes for anti-bribery and corruption efforts. We should expect this trend to continue. R&C

PERSPECTIVES

THE MODERN SLAVERY ACT 2015

BY **SIMON OSBORNE**
> ICSA: THE GOVERNANCE INSTITUTE

The UN International Labour Organisation's global estimate of forced labour in 2012 placed the number of people trapped in various forms of slavery throughout the world at 21 million, of whom 78 percent toiled in forced manual labour, 22 percent were trapped in sex slavery and about 26 percent were children. More recent estimates place the number at around 45 million.

These are shocking statistics in the 21st century and this is one of the reasons why the Modern Slavery Act 2015 was introduced by the then home secretary, Theresa May, to ensure that companies are not complicit in this insidious multi-billion pound industry.

A recent review of the Act found that 289 modern slavery offences were prosecuted in 2015 and that there was a 40 percent rise in the number of victims referred for support. Despite this, the UK Home Office estimates that there are between 10,000 and 13,000 potential victims of slavery in the UK.

Definition of modern slavery

The term 'modern slavery' covers slavery, servitude, forced and compulsory labour and human trafficking. A typical example is a migrant worker who has taken a loan to pay for travel to another country to work or to pay fees to an organisation that finds them work (or both), with the intention of repaying the loan from their earnings.

They then become trapped in a situation where other amounts are added to the loan while they are working for things such as accommodation or transport and they are unable to meet the loan repayments from their earnings. Frequently their passports are also taken from them and held by their employer.

Konstantin Sasmurin and Linus Ratautas were jailed in January this year for three and half years for trafficking twin brothers from Lithuania and forcing them to work in food processing factories in Suffolk. Rescued after four months in the clothes they arrived in after living at an address that had no beds and with mould on the walls, the victims received £20 in total between them for the work that they did – between July and October 2013 – after being forced to provide Sasmurin and Ratautas' contact and bank details to their employers. Such stories

show why companies need to understand the risks involved in employing people about whom they know little.

Section 54 of the Modern Slavery Act 2015 provides that: "A commercial organisation… must prepare a slavery and human trafficking statement for each financial year of the organisation". Effective from 31 March 2016 (as set out in the Transparency in Supply Chains Guidance rather than the Regulations), all organisations with a year end of 31 March need to produce a report "as soon as reasonably practicable", preferably within six months of 31 March 2016, covering the previous financial year and annually thereafter.

Organisations affected by the Modern Slavery Act 2015

Affected organisations include all companies and partnerships, or subsidiaries of a group structure, wherever they are incorporated or established, that satisfy the following qualifying requirements: (i) have a turnover of £36m or more (over the entire organisation including parts of the business outside the UK); (ii) that supply goods or services; and (iii) that carry on at least part of their business within the UK – referred to as having a "demonstrable business presence in the UK" (this is a question of fact and a common sense approach should be taken to this).

Organisations that do not have a "demonstrable business presence in the UK" will not be caught – even if they have a subsidiary in the UK (provided, of course, the subsidiary is not carrying on business in the UK). However, even where neither the group as a whole nor any part of the group meets the qualifying requirement, the organisation needs to be aware that it may form part of another group's supply chain so will need to assess this risk.

> **"Companies need to produce a statement describing the steps they have taken during the financial year to ensure slavery and human trafficking are not happening."**

The devil is in the detail

Companies need to produce a statement describing the steps they have taken during the financial year to ensure slavery and human trafficking are not happening in any part of the business or supply chain. This statement needs to cover the entire business, including steps taken in relation to foreign subsidiaries which are part of the business or supply chain, whether or not these parts

of the business are caught by the Act individually – particularly if the foreign subsidiary is operating in a high-risk industry or location.

An article in The Independent newspaper in 2012 exposed how difficult it is for companies to monitor supply chains in developing countries where "labour laws are lax and people are desperate for jobs". India has the largest number of people in slavery in the world (approximately 14 million) and Mauritania has the highest percentage of its population in slavery (4 percent). It is difficult for companies to ensure that all of their suppliers' employees are making widgets of their own free will or earning a decent wage when the odds are stacked against them numerically.

If a subsidiary operates independently of a group and is not itself caught by the Act, there is no obligation to include that subsidiary as part of the business or supply chain, but the guidance encourages parent companies to include these subsidiaries on a voluntary basis.

There is no prescribed format for the general layout of the statement or the level of detail included. However, the guidance indicates a preference for simple, succinct statements with links to other policies and documents. This statement may include information about the organisation's structure and business supply chains and, where there is a risk of slavery and human trafficking, steps taken to assess and manage the risk (including senior management oversight of risks); relevant policies and due diligence processes; training made available to staff; and the effectiveness of all the measures taken within the business and supply chains, measured against key performance indicators (KPIs).

The suggested information that may be included is not prescribed. Organisations can comply with the requirements of the Act by making a statement that no steps have been taken to deal with slavery and human trafficking but this would clearly cause reputational issues.

It is expected that annual statements will show progress and improvement in tackling these issues over time. Therefore, it is advisable for companies to focus on processes, policies and procedures rather than guarantee supply chains are free from slavery and human trafficking.

Organisations should verify all information included in the statement to ensure accuracy and ensure it will stand up to scrutiny. This statement must be approved by the board (or equivalent body for partnerships) and be signed by a director. The signed copy of the statement will need to be made available on the company's website with a link to it in a prominent place on the home page. Where the provisions of the Act apply to both the parent and a subsidiary, only one statement by the parent is required on behalf of both.

Preparation is key

Gathering the necessary information and assessing the risks could be a complex exercise, particularly

for large, multinational supply chains. 'Supply chain' is not defined in the Act but the guidance states it has its everyday meaning. Organisations will need to engage with their suppliers to gain assurances and ensure they understand any risks posed by the supplier's operations – and their sub-suppliers.

They will need assurances from their suppliers in relation to the sub-suppliers further along the supply chain. Organisations should not overlook suppliers that could be a particular risk such as those providing low paid, unskilled labour or third-party recruitment agencies. Supplier agreements and contracts may need to be reviewed and amended. Joint ventures and outsourcing should also be assessed, and acquisitions could also pose a risk so compliance with the Act should also be included in due diligence carried out.

Organisations should offer training for staff. They should review policies, procedures and processes and amend where necessary. This should include procurement and supply, recruitment, whistleblowing, grievance procedures and loan agreements, and check their insurance covers risks identified. They should also set out what would happen if slavery or human trafficking is discovered.

Theresa May has pledged to lead the fight against modern slavery, setting aside £33m to fight it in the UK. There are limited penalties for non-compliance but the disclosure duty is subject to enforcement by the Secretary of State by injunction. This is unlikely to happen in practice but the biggest risk to organisations is reputational. As Mrs May said in her foreword to the guidance: "It is simply not acceptable for any organisation to say, in the twenty-first century, that they did not know. It is not acceptable for organisations to ignore the issue because it is difficult or complex. And, it is certainly not acceptable for organisations to put profit above the welfare and wellbeing of its employees and those working on its behalf." Expect pressure groups to be monitoring compliance and highlighting any non-compliance. R&C

Simon Osborne
Chief Executive Officer
ICSA: The Governance Institute
T: +44 (0)20 7612 7001
E: ceo@icsa.org.uk

ONE-ON-ONE INTERVIEW

DEVELOPMENTS IN REGTECH

Garrett Gafke
President & Chief Executive Officer
IdentityMind Global
T: +1 (650) 618 9977
E: garrett@identitymind.com

Garrett Gafke is a successful entrepreneur and Fortune 500 executive, blending early stage action with public company knowledge. Prior to founding IdentityMind Global, Mr Gafke served as president & CEO of Paymate, an innovative provider of payment and risk management services that was acquired by Flexigroup (FLX). He has a proven track record of founding and growing great technology companies, having completed five M&A transactions, and two successful IPOs. Mr Gafke is an active angel investor and board member of early stage companies around Silicon Valley.

RC: In broad terms, what do you consider to be the most significant developments to have taken place in the regulatory technology (RegTech) space over the past 12 months or so?

Gafke: There have been a number of significant developments affecting RegTech. First, the explosion of FinTech has helped large financial institutions as well as brand new firms. They, in turn, provide greater access to financial services, especially to the underserved. Second, there has been an acceptance that tech can solve regulatory issues, not just fraud but traditional back-office regulatory concerns for start-ups as well as large financial institutions. Third, automation has become a driver of compliance efficiencies, with small firms scrambling to automate so they can scale efficiently and large firms automating to become better. Finally, the use of a tremendous amount of Big Data is helping to prevent and detect fraud, money laundering and financing of terrorism.

RC: What are some of the common issues facing businesses that RegTech seeks to address?

Gafke: Companies are grappling with how to automate existing processes and procedures. With so much data available and the ability to process and analyse complex data scenarios in real-time, businesses must determine how to operationalise the data so it can better inform their processes. Companies are also trying to figure out how to make use of the data available. Traditional financial organisations tend to function in silos, with the compliance team separate from the risk team and so on. A common data taxonomy allows different groups to use and share data across the organisation. In addition, companies are seeking to leverage data outside of their own four walls. There is no easy way to leverage industry data across players. Finally, companies face uncertainty in regulations. Existing regulations have not caught up with new models, innovators are trying to stay ahead, but no company wants to be the first to receive regulatory fines.

RC: Could you provide an insight into the kinds of RegTech tools and solutions that are available? To what extent do they increase the efficiency of regulatory compliance monitoring and risk reporting?

Gafke: RegTech tools can be divided into four areas. The first is reporting and analytical tools which provide the ability to record activities that are easy to audit and improve processes. Analytics can also help uncover complex scenarios faster. The second category is evaluating applicant risk or identifying digital identities. These tools can expand the reach

of financial services while providing intelligence about the potential clients. The third category is placing risk models on top of transaction monitoring to detect suspicious activity. These tools help uncover complex scenarios in real time, and detect and prevent financial crimes in real-time while meeting regulatory guidelines with enough certainty increases confidence in undertaking business models that are more disruptive. The fourth category is automating anti-money laundering compliance, such as sanctions screening. As financing of terrorism becomes more pervasive, more pressure is applied by regulatory bodies to analyse clients and their associations. This has become a operational burden that can be largely automated with better data capture and analysis.

RC: In your experience, what challenges might companies encounter when integrating a RegTech solution into their existing systems? What steps can they take to mitigate potential problems?

Gafke: If you think of systems as only technology, these challenges might cover integrating into existing systems and processes, including the availability of Application Programme Interfaces (APIs) to leverage and share data between systems, scalability that allows new and old systems to keep up with transaction volume as data is shared, and flexibility that allows purchasers to match their processes across their new and old systems. If you think of systems as including the old manual and people-driven processes, then those challenges include deciding when to use manual and automated processes, syncing up manual and automated processes for maximum efficiency, and how to incorporate alerts and case management for optimal handoffs. Mitigating these problems ultimately revolves around understanding your desired end-state and ensuring that the chosen RegTech solution fits with your existing business systems, infrastructure and people processes to get you there.

RC: To what extent do RegTech and Big Data complement one another when companies are searching for an effective regulatory programme? Can this go further, and actually transform regulatory compliance into a competitive advantage?

Gafke: RegTech and Data/Big Data work hand in hand. The best RegTech solutions will capitalise on the knowledge provided by Big Data to solve existing problems better, faster and cheaper. Regulatory compliance is already a competitive advantage for certain firms; it is their secret sauce. FinTech firms like Airbnb or Stripe have built new systems from the ground-up specifically for their use-case, however even those need more advanced capabilities as the models have evolved. These systems have been

built with (APIs) to get data in and out, scalable architecture to support the use of Big Data, and tools that allow data scientists and fraud analysts to work hand in hand detecting and mitigating risk.

RC: What advice would you give to companies considering RegTech to satisfy their regulatory compliance obligations?

Gafke: Software is a great way to help meet your compliance obligations. However, software is the easy part. To successfully implement solutions it is critical to have a number of factors in place. The first is buy-in. From the executives down to audit departments, there should be use cases explaining how this technology will work. None of these companies should think they have it all covered and need to keep pressing for even incremental enhancements within their process or platform. What operations it will change, etc. Deployment cannot be done in a vacuum. The second factor is strong data architecture. Legacy systems can stop RegTech solutions before they begin. The willingness to move to an internal data architecture that supports efficient processes and technology is paramount. The third factor is operational workflows. The hardest aspect is to come up with good strategies and technologies to make these processes efficient. But if the starting point is weak, technology will not help. Finally, companies need to work with regulators and the industry. Be part of the solution and understand that transition takes time, especially in larger financial institutions.

> **"Regulatory compliance is already a competitive advantage for certain firms; it is their secret sauce."**
>
> *Garrett Gafke, IdentityMind Global*

RC: Going forward, do you believe regulatory regimes and policies will be influenced by a more widespread use of RegTech, and develop in conjunction with its adoption?

Gafke: It is no doubt the case that regulators will look at RegTech technology as they consider new regulations and changes to existing rules. Understanding the strengths and weaknesses of

the technology provides regulators with greater guidance on what is possible and what may not be. It also provides direction to regulators on where they may be able to encourage the use of more effective technologies like digital identities while discouraging older, less effective technologies or processes. This is no different than any other discipline. The beginnings are slow, but ultimately they inform each other, and adoption becomes the norm – on both sides.

RC: Over the coming months and years, what particular trends and developments do you expect to emerge in this space? Is the increased prevalence of RegTech as a regulatory compliance option inevitable?

Gafke: The genie is out of the bottle. There may be missteps, but for both companies and regulators the use of RegTech will become so commonplace that the term RegTech will be replaced. It will just be considered regulation. Here is why: firms love it. They love it because of the scalability, cost and speed. The changes do not require data centres and months to complete. They also love the flexibility. RegTech provides flexibility that typically only start-ups with strong coders have. This is nirvana, especially for compliance analysts at large financial institutions that typically deal with technology that is 10-plus years old and does not communicate with other systems they have to use. Examiners and regulators love RegTech because companies can do more. They can do more reporting, more analysis and be more efficient. Retrieving and using relevant data can be accomplished in real time. They can also provide better services. Companies can use this technology to expand services to the underserved and expand the financial health of customers. RC

PERSPECTIVES

BREAKING THE RISK GLASS CEILING

BY **JULIA GRAHAM**
> AIRMIC

Despite high profile failures of risk management in recent years, the cost and probability of failure is often underestimated internally and externally, including the time required to fix the problem.

Risk taking remains a fundamental driving force in business: when managed correctly it drives competitiveness and profitability. However, when managed unsuccessfully, the results can be devastating.

The role of senior management in ensuring companies manage their risk successfully is of critical importance. Encouragingly, this is increasingly recognised in official guidelines. The Financial Reporting Council's risk guidance published in October 2014 stated that the board should take "ultimate responsibility for risk". And the FRC's most recent risk guidance, 'Corporate Culture and the Role of Boards' published in July, states that senior executives should "get out of the boardroom" to understand how their firms are behaving.

The importance of this is backed up by research we commissioned, published in 2011 entitled 'Roads to Ruin', which studied the underlying causes of high-profile corporate crises which left the company reputation in tatters. One trait common to almost all case studies was 'board risk blindness' which resulted from a 'risk glass ceiling'. In other words, risk information did not flow freely up to senior management, usually due to cultural and structural

barriers. The result was a failure of the board to properly recognise and engage with risks inherent in the business, including risk to the business model, reputation and their 'licence to operate'.

Recognising if your company suffers from board risk blindness is not always easy and it requires coordination across the company. Our latest research indicates that the interface between functions on risk management and education in risk management across the organisation is still not as mature as it might be. But there are red flags to look out for. For example, two of the key indicators for assessing board risk blindness are tracking how and when people speak up and how their words are responded to, and how risk responsibilities are embedded in role responsibilities and reward systems. Given the lateral gap in the penetration of risk management, it might therefore be more accurate to describe the risk glass ceiling to include risk glass walls.

Furthermore, lessons can also be learnt from the most successful organisations. In follow-up research, 'Roads to Resilience', released in 2014, researchers found that the key to achieving resilience is to focus on behaviour and culture. This led to re-thinking and challenging prevailing attitudes towards risk and re-thinking traditional risk management techniques which, while important, do not in themselves create a culture of resilience.

Although the case study organisations were very different, five common principles of resilience emerged. These are: (i) risk radar – the ability to anticipate problems and see things in a different way; (ii) resources and assets – diversified to provide opportunities to respond to opportunities; (iii) relationships and networks – free flowing risk information prevent 'risk blindness'; (iv) rapid response – people and processes are in place to manage crisis or disaster; and (v) review and adapt – learn from experience including near-misses.

> **"Recognising if your company suffers from board risk blindness is not always easy and it requires coordination across the company."**

These principles enable a culture based on trust and respect, one that has a high level of risk awareness to identify trends and correctly analyse, evaluate and respond to risks and thereby avoiding board risk blindness.

Risk culture is not new but it has gained traction and importance as a concept since the financial crisis. Risk culture is dynamic. It can be a mixture

of formal and informal processes and may exist in more than one form. However, it is important that risk culture is set within the overall framework of the organisation's vision, mission, corporate culture and risk management system. And most importantly, it comes from the boardroom.

The context of globalisation, the challenges of operating in the digital economy, the pace of change and the increasing complexity and aggregation of risks, are undoubtedly combining to place more demands on boards. The good news is that achieving a resilient risk culture is not just about avoiding the next disaster. Our research found that the qualities embedded in resilient organisations help them succeed in other respects, including profitability and shareholder return.

As Sir Winfried Bischoff, Chairman of the FRC, states in the foreword to the latest FRC publication: "A strong culture will endure in times of stress and mitigate the impact. This is essential in dealing effectively with risk and maintaining resilient performance." A healthy culture protects firms, enabling organisations to deal more effectively with both the expected risks and the unexpected ones. Resilience consequently should be at the heart of strategy and business model in every organisation.

The next step for the risk community is to further understand the 'why, what and how' of risk culture and to develop standards for best practice in the assessment, measurement and reporting of this complex subject. RC

Julia Graham
Deputy CEO
Airmic
T: +44 (0)20 7680 3088
E: julia.graham@airmic.com

MINI-ROUNDTABLE

REPUTATION RISK MANAGEMENT – THE IMPORTANCE OF EFFECTIVE ETHICS POLICIES

PANEL EXPERTS

Andy Reisman
Senior Manager
Ernst & Young LLP
T: +1 (617) 585 0302
E: andrew.reisman@ey.com

Andy Reisman is a senior manager in EY's Fraud Investigation and Dispute Services practice, focusing on business integrity and corporate compliance. He has previously served as a chief compliance officer of a global services company and as general counsel of a global business of one the world's leading companies.

Dan Casciano
Principal
Ernst & Young LLP
T: +1 (336) 210 2740
E: daniel.casciano@ey.com

Dan Casciano is a principal in the Advisory Services practice of Ernst & Young LLP and has more than 25 years of experience in risk and advisory services. He leads EY's Risk Enabled Performance Management National Practice for the United States. Mr Casciano has directed numerous enterprise risk and compliance programmes and enables them through governance, risk and compliance technologies.

John Rogula
Senior Manager
Ernst & Young LLP
T: +1 (312) 879 2379
E: john.rogula@ey.com

John Rogula is a leader in the Advisory Risk Transformation Services practice of Ernst & Young LLP and is the Americas Enterprise Risk Management Practice and Healthcare Own Risk and Solvency Assessment Lead. He has more than 25 years of experience in management consulting with a diverse background in governance, risk and compliance, enterprise risk management, IT strategy, organisational strategy and programme management.

RC: How would you characterise the importance of a company's reputation in today's business world? To what extent are risks increasing that could damage those reputations?

Reisman: We are seeing businesses impacted by a multitude of disruptive forces and megatrends globally, each requiring a different response to manage the associated risk. Organisations are challenged with developing a comprehensive view of risk, as well as regularly identifying and responding to existing and emerging risks. We expect and are seeing organisations make investments in their risk management capabilities not just to protect the organisation, but also to create value. Mature risk management recognises that the rapidly changing risk landscape not only creates challenges, but also presents opportunities. Organisations that manage risk well are better positioned to capitalise on the upside potential of risk.

RC: In your experience, are companies in general doing enough to safeguard their reputations against the many threats they face?

Rogula: From our 2015 governance, risk and compliance survey research, we concluded only 61 percent of respondents are using some form of risk monitoring to identify trends or risks that may impact their organisation's business strategy and reputation. Companies are looking to develop risk management frameworks that enable them to shift their focus with regard to how they identify and respond to the reputational risks they face, with both positive and/or negative impacts, and best respond to each risk appropriately. Let us look at the example of social issues – to safeguard against a social issue, organisations should internalise the issues to ensure commitment and consistency to social performance. Additionally, the organisation needs to establish capabilities to monitor, detect and respond to social media, both positive and negative.

> **"Mature risk management recognises that the rapidly changing risk landscape not only creates challenges, but also presents opportunities."**
>
> *Andy Reisman, Senior Manager*

RC: What are the key benefits to integrating ethics, values and transparency into an organisation's leadership and culture?

Casciano: Shared principles and honest communication builds trust – an essential element of an effective organisation. Trust empowers employees to challenge the status quo, innovate and confront risks. Unspoken and powerful values guide difficult decisions. Employees can represent the organisation – openly and genuinely – to customers, investors and the public, encouraging honest communication back from those stakeholders and building strong relationships. Of course, ethics, values and transparency keep an organisation out of trouble; frauds typically do not grow in the sunlight.

RC: What role can an effective ethics policy play in creating a resilient and sustainable organisation? In practical terms, how should such a policy be disseminated throughout an organisation?

Reisman: The 2013 COSO Internal Control – Integrated Framework addresses this point well. Principle one requires an organisation to demonstrate 'a commitment to integrity and ethical values'. The ethics policy is a formal statement of that commitment. It is supported by management 'directives, actions and behaviour' that create an ethical tone at the top. The policy is a basis for the organisation's board of directors to hold management accountable. In most companies, a code of conduct communicates the organisation's ethics policy and standards of conduct. It also describes employees' rights and responsibilities to speak up about unethical behaviour. An organisation should have a compliance and ethics programme to support the code, with training, risk assessment and enforcement of standards of conduct. Effective communication means listening as well as speaking; an employee survey can indicate whether the policy's words reflect the message communicated through management's actions. The best way for leaders to

> **"Trust empowers employees to challenge the status quo, innovate and confront risks."**
>
> *Dan Casciano, Principal*

disseminate a code of conduct is to use it with their teams. They should discuss the principles that guide their decisions and foster shared values.

RC: To what extent does the prevalence of social media add to the difficulties facing organisations when they are looking to build and protect their reputation?

Rogula: With the transparency of information, and the speed at which information is spread through social media, the potential for a reputational impact has increased. Information can quickly be disseminated to the masses with little filtering and validation of the information. Social networks give the opportunity for consumers,

competitors and organisations themselves to spread both positive and negative information about a company or experience to a vast number of social followers. In 2014, the ALS Association successfully leveraged the social media platform to encourage donations and build its reputation. During an eight week period, individuals used social media to challenge each other to have buckets of ice water dumped on their heads to promote awareness of ALS and to encourage donations for research. The social media event led to more than 2.4 million tagged videos on Facebook, and raised over $115m, enabling significant progress in advancing ALS research.

RC: What advice can you offer to companies in terms of establishing policies and procedures to manage reputational risk?

Casciano: Reputation needs to be considered in the assessment and prioritisation of risks. We recommend companies focus on five impacts that risks can have to an organisation, and incorporate these into the development of their risk tolerance and risk response strategies. These impacts include financial, operational, strategic, legal and regulatory compliance, and reputational. It is this holistic account of risk impact that enables a company to fully understand the magnitude of the risk in relation to its risk tolerance, and to determine the appropriate resources to apply to mitigating the risk through proactive and reactive risk response strategies. The assessment of risks cannot be very effective as an annual, point-in-time account of risks. Reputational risk management needs to be integrated with business processes and reviews,

> **"Social networks give the opportunity for consumers, competitors and organisations themselves to spread both positive and negative information about a company."**
>
> *John Rogula, Senior Manager*

and conducted on a frequent basis. Our research shows that organisations have made a significant amount of progress in bridging the gap between risk management objectives and business objectives. But less than 16 percent of those organisations surveyed feel the risk processes are embedded in the business process and aligned with the organisation's strategy.

RC: How do you envisage reputational risk management evolving over the coming years? Do you expect companies to focus more attention and resources on this area?

Reisman: Over the last five years, organisations have improved the way they identify, manage and respond to risk. They have created executive-level roles to provide risk oversight, established functions to deal with complex legal and regulatory requirements and implemented supporting technologies to recognise risk exposures. Reacting to increased market volatility and regulatory changes, organisations have renewed efforts to enhance their internal controls. With a renewed ERM framework focus by regulators and commissions, such as OMB Circular A-123, NAIC's ORSA Model Act and the COSO ERM Refresh, organisations will need to continue to demonstrate progress in the management of risks, and take advantage of opportunities to drive performance. R&C

PERSPECTIVES

VISIONARY BOARDS: GOVERNING COMPANIES THROUGH GLOBAL DISRUPTION

BY **SUSAN STAUTBERG**
> WOMENCORPORATEDIRECTORS FOUNDATION

With 41 percent of global CEOs expecting their companies to be transformed into a significantly different entity in the next three years, according to KPMG's '2016 Global CEO Outlook', corporate boards face the challenge of preparing themselves for risks they may not even be aware of. Economic and geopolitical uncertainty, transformational technology, changing demographics, business model disruption and new competitors: each change poses new opportunities, but also new threats to the very sustainability of a company.

In times of drastic change, there may be a corporate tendency to play it safe. Plans to move into new markets may be tabled until political situations quiet down, or investment in new technology held off to avoid committing to systems that may be outdated in a couple of years. And, to withstand severe market and revenue fluctuation, company boards must keep an even closer eye on financial risk management to keep the lights on. The oversight function of a board may indeed need to go into overdrive.

But rather than retreating to safety, these periods of uncertainty are the exact times when boards need to stretch the most – to think far beyond the present and reimagine what a company can be five, 10, 20 years hence. How can boards deliver beyond their

oversight role, and provide the kind of governance a company needs to move toward a very different future?

Recently, the WomenCorporateDirectors Foundation's Thought Leadership Commission teamed up with KPMG's Board Leadership Center to explore what it takes to make a board future-focused. The Commission gathered more than 30 corporate board members and governance advisers as thought leadership commissioners for discussions around this issue, drawing from the combined many decades of board experience from this diverse, global group. The resulting report emphasised the value of a 'visionary' board: "Boards must get the basics right – oversight of risk and selection and oversight of company leadership", says the report. But, in addition, boards "add significant value when they also move toward the visionary", when they excel at not only providing oversight and insight, but foresight.

What is it that makes a board visionary? The report, 'Seeing Far and Seeing Wide: Moving toward a Visionary Board', argues that visionary boards have a "focus on the future, expansive thinking about the implications of changes in the external environment, and creation of a culture that enables the organisation to achieve desirable change".

The ability of a board to adapt nimbly to transformations is critical to managing the inherent risk around any sort of change – whether the change is economic, regulatory, financial, technology-driven,

etc. As Jack Welch said, "If the rate of change on the outside exceeds the rate of change on the inside, the end is near." For directors, this means a constant assessing and reassessing of the external factors that may impact the company long-term. Technology and consumer behaviour changes serve to blur the lines between industries, allowing companies to jump 'lanes' into different sectors and become a new competitor (Amazon and Apple are two that are doing this well). Economic and political crises throughout the world (from Brexit to Brazil) have regulatory, trade and market implications for what may be decades to come. Visionary boards see these events and ask their management teams: how does this affect us? What strategic shifts must we make as a company to mitigate risk but also to jump on possible opportunities?

And it's not just about seeing the larger trends. Visionary boards anticipate disruption by seeing the 'weak signals' that other companies might not be picking up on yet. Maggie Wilderotter, a director at Costco, DreamWorks, Hewlett Packard and Juno Therapeutics, explains that boards need visionary leadership – "individuals who can see not only what's happening now, but can see around corners to anticipate what's coming".

To ensure that one's board has the people around the table to pick up on weak signals in the market, boards must be expansive in their thinking. Nominating committees have a key role in bringing diverse perspectives onto the board – whether in

expertise, industry, geography, gender, ethnicity or age. A director from overseas can offer valuable insight about a new market – both positive and negative. Those from a different industry can advise how technological changes disrupted one sector and could well disrupt others. Directors of varying ages and ethnicities can disabuse boards of incorrect assumptions about consumer patterns and expectations. This kind of valuable insight that digs beyond today's headlines will keep boards more knowledgeable, insightful and forward-thinking when they apply this insight to corporate strategy.

As boards interact with their management teams, asking the right question at the right time – and then asking the second and third question after that – is integral to management's being able to develop plans to address a concern before it becomes a problem. Estelle Metayer, a director at Ubisoft Entertainment SA and at BRP (Bombardier Recreational Products) Inc., says that an important role of the board is in pointing out management's blind spots. Has management fallen in love with an acquisition in a country where it does not have sufficient understanding of the marketplace? Is the focus so strongly on short-term results that compliance is at risk?

Ultimately, these kinds of expansive, forward-thinking questions are what boards have a responsibility to ask as part of good governance. A visionary board is really the periscope of a company, providing management with sightlines toward a surer route, even through the inevitable choppy waters that are the new normal in today's world. R&C

> **"Those from a different industry can advise how technological changes disrupted one sector and could well disrupt others."**

Susan Stautberg
CEO, Co-Founder and Co-Chair
WomenCorporateDirectors Foundation
T: +1 (561) 290 0389
E: sstautberg@womencorporatedirectors.com

PERSPECTIVES

CHANGE A RISKY BLUE-SKY STRATEGY INTO A FISCAL VISION WORTH ITS WEIGHT IN GOLD

BY **GARY W. PATTERSON**
> FISCALDOCTOR

It is hard to be vigilant against being blindsided in a world of paradigm-shifting events if even part of your strategy process suffers from blue-sky syndrome. Strategies without a fiscal vision are not grounded in reality. Implementing back to the basics fiscal vision improvements can rapidly and inexpensively reduce strategic, financial or operational risks.

Where can you improve the emphasis from crafting impressive-sounding mission statements, core values and new initiatives with scant consideration given to the company's real financial position?

Going deeper, how often have you seen strategic planning fail because it has no connection to reality or the company's current conditions – or, most disheartening, no connection to management incentives and bonus plans? How many companies in year three, four and five of a five-year strategic plan just plug in the same financial assumptions articulated in an older plan? Where could your executive team better describe bottom line performance based on a review and analysis of the financial statements, budgets and financial projections?

Objectively reviewing your company's financials helps determine whether your current strategy

is working or not. Actual numbers sometimes reveal an underlying reality vastly different from how the executive branch wishes to perceive company performance. If the numbers indicate that the company is not going to reach financial and budgetary goals, no pie-in-the-sky strategy is going to help it maintain its competitive advantage, much less sustainably grow profitably. In the end, business is all about cash in the bank, valuable assets, wise investments, a balanced balance sheet, realistic budgets and financial projections – with a sound strategy supporting the bottom line.

Fiscal vision, defined

A fiscal vision makes your strategic game plan measurable so at any point in time you and your executive team can ascertain if and how your company is achieving its strategic goals in accordance with your financial objectives. To this end, apply fiscal vision to the four most critical drivers of any business: risk, opportunity, change and uncertainty. The first two aspects (risk and opportunity) focus on internal forces that determine a company's gestalt (that is, its business orientation and management mindset). The latter two aspects (change and uncertainty) focus on how a company responds or reacts to external forces (i.e., the economic environment) in which it operates.

The risk driver

Review and analysis of your current financial position provides management a better understanding of how well strategy supports the amounts and types of risk currently being undertaken. Going forward and integrating your strategic vision and fiscal vision will enable your organisation to better know how much risk it is taking.

A strategic vision with a fiscal focus will allow your company to feel more comfortable that its risk strategy is realistic, prudent and even doable, rather than suddenly realising too late that you have bet the farm for too little reward.

A company's periodic review of particular issues can better define the company's relationship to risk. Update your definition of risk *vis-à-vis* the company's historical financial statements. Describe the company culture's attitude (averse or friendly) to risk. Review, or establish, an acceptable risk/reward trade-off. Accept the level of risk necessary to reach short, intermediate and long-term financial goals. And align a risk level (low, medium or high) to your company's infrastructure, operations and management mindset.

The opportunity driver

Where can you better consider opportunities after analysing two important base-line figures – revenue and net income? Far too many financial

projections show revenues starting one quarter earlier than will actually occur, and expenses starting one quarter later than will actually occur. Brainstorm what opportunities to pursue in earnest after management determines and agrees on the company's bottom line goal.

Potential opportunities in the marketplace need to be examined as to their impact on intermediate (next year) and longer term (two to three years out) current revenue and net income. The risks associated with these opportunities needs to be understood and evaluated in the context of the firm's long term growth and sustainability. Gains, losses and risks associated with each opportunity require clarification. The corporate financial position should be re-inspected with an eye toward the pursuit of priority opportunities.

The change driver

Most companies, whether they admit it or not, know whether they are leaders or laggards (and in some cases, has-beens) when it comes to foreseeing and adapting to change. When was the last time top management willingly and thoroughly put your business model under a microscope to determine where viability and relevance can be improved?

Imagine the benefit of reviewing key issues for maintaining or achieving an industry leadership position. Which business model's critical factors could that improve: pressing issues and concerns; the availability of resources, including human resources; pursuit of short term and long term opportunities; presence of short term and long term risks; or procurement of current and future financial resources to address the most immediate concerns, opportunities and risks?

The uncertainty driver

The world economy continues to change at warp speed. Without ongoing introspection, you have even less control over external forces that continuously threaten market share and competitive positions. Globalisation, climate warming, wars, social unrest, poverty, technological advances, epidemics and natural disasters are just a few of the forces affecting the performance (and bottom lines) of most companies. Industries today are operating under the tremendous pressure of forces outside of their control. Where are you taking risks, wittingly or unwittingly, or making decisions that could do irreparable damage to your company? Nowhere is the adage "haste makes waste" more relevant than it is in today's business climate. The risk of doing business in any industry is greater today precisely because companies are forced to move at a faster clip, making quick decisions judged with hindsight. Reckless decisions have serious consequences.

That is why contingency planning is a must. You do not have to go far back in time to recount what happens to companies that cut corners. Profits and reputations tank overnight. BP, Toyota and Bears Sterns are just a few stunning examples of companies that bet the ranch because they felt they were invincible, or at least immune to disaster. Only after companies like these fall from grace do we question how much of their strategies and financial goals included self-serving roadmaps. What is missing in most failed strategic plans is the lack of a contingency plan. It keeps a strategy on the straight and narrow and management focused on the health and well-being of the business.

> **"To improve the usefulness and effectiveness of your fiscal vision strategy, develop a contingency plan that addresses likely scenarios over the next three to five years."**

To improve the usefulness and effectiveness of your fiscal vision strategy, develop a contingency

plan that addresses likely scenarios over the next three to five years. Until management is willing to come to grips with the external forces that threaten to destabilise the company, all the carefully crafted strategies are for naught. To this end, the final brainstorming session should focus on developing a companywide contingency plan.

Contingency planning should also include issues like identifying potential doomsday scenarios for the company, preparing for likely catastrophes, developing safety measures and precautions to ensure likely catastrophes do not happen, and improving the quality of financial resilience to absorb a likely catastrophe. Who out there is working feverishly to make your well-earned success next year's Kmart? How well does your contingency plan consider these issues?

Putting the fiscal vision to work

Today's economy remains a perfect storm of rapid change, risk, opportunity and uncertainty. Those executives who come to grips with the financial reality driving their organisation's performance and business objectives will be in a far better position to lead their industries in new and exciting directions. But embracing such a reality is not for the faint of heart. What is required is a willingness to build (and in some cases rebuild) your strategic plan around a fiscal vision. In the end, a strategy that is driven by the company's financial performance and goals is a strategy that will separate the victors from the victims. These basics are hard work to maintain. What does your strategy say about the future of your company? Where might some of the preceding basic tweaks earn your story a business Emmy? R&C

Gary W. Patterson
Founder
FiscalDoctor
T: +1 (678) 319 4739
E: gary@fiscaldoctor.com

PERSPECTIVES

AN OVERVIEW ON DIRECTORS' DUTIES AND LIABILITIES IN SAUDI ARABIA

BY **NABIL ISSA, JAMES STULL AND SAYF SHUQAIR**
> KING & SPALDING LLP

On 2 May 2016, the new Companies Regulations were introduced in the Kingdom of Saudi Arabia to replace the previous regulations that were implemented in Saudi Arabia over 50 years ago. In general, the new regulations have been well-received and are seen as a step forward in the modernisation of the regulatory and investment landscape in Saudi Arabia, consistent with recent developments such as the opening of the stock market to foreign investors. The new regulations provide clarity and address several concerns regarding corporate structuring, ongoing operations and reporting obligations. One particular area that the legislator sought to strengthen was the role of managers and directors by placing additional responsibilities and obligations on them (and in some cases harsh penalties), in line with Western jurisdictions, in order to protect the wider interests of the stakeholders involved. In this article, we take a detailed look at managers' and directors' duties and liabilities in limited liability companies (LLCs) and joint stock companies (JSCs) in Saudi Arabia as stipulated under the new regulations.

Limited liability companies

The LLC is by far the most common corporate vehicle in Saudi Arabia. Its attractiveness generally lies in its ease of formation and the relatively

limited ongoing regulatory and reporting obligations which it has to abide by. In addition, although the new regulations set forth the general framework applicable to LLCs, shareholders in LLCs are given broad discretion to agree on various matters pertaining to the business and operations of the company, which are set forth in the company's articles of association.

One of the matters over which shareholders have considerable discretion is the management structure that is to be adopted by the company. Shareholders may opt for either a single manager or a board of managers to manage the company, each having its own practical considerations. Also, shareholders are given some discretion to agree on the scope

and breadth of the duties, subject to the statutory requirements in the new regulations.

Under the new regulations, managers' duties primarily involve straightforward reporting and disclosure obligations, particularly in relation to the preparation and submission of financial statements. The new regulations do not provide an exhaustive list of duties for managers of LLCs, which are usually set forth in the articles of association, but instead they stipulate that managers shall be held liable for any loss suffered by the company or the shareholders or third parties as a result of the managers' violation of the companies regulations and the company's articles of association. This approach is generally in line with the position adopted under the previous regulations where managers were subject to a similar liability threshold.

However, under the new regulations, managers have an additional burden to exercise extra diligence when managing companies with questionable financial health. The new regulations provide that if an LLC's losses reach 50 percent of its paid-in capital, the managers shall record such losses in the commercial register and convene a general assembly meeting within a period not exceeding 90 days from the date of becoming aware of the losses to discuss the continuance or dissolution of the company. Further, the new regulations impose significant penalties and provide that a manager, officer or member of board of directors shall be subject to imprisonment for a term not exceeding five years and a financial penalty not exceeding SAR 5m (or both) in case they did not convene a meeting of the shareholders or general assembly or have not taken the necessary steps to address the situation upon becoming aware of the losses.

> **"Under the new regulations, the maximum penalty provided for directors in a JSC has substantially increased to become imprisonment."**

Joint stock companies

A JSC is a more heavily regulated entity than an LLC, and is akin to a corporation in Western jurisdictions. While the shareholders in a JSC have the discretion to agree on certain matters in the company bylaws (which is the equivalent of an LLC's articles of association), the new companies regulations also govern a significant number

of operational and managerial aspects. A JSC previously needed to be formed by a minimum of five shareholders, but under the new regulations, generally a minimum of two shareholders is required, and in fact, single shareholder JSCs can be formed by the government, public institutions, wholly-government owned companies and companies with capital not less than SAR 5m.

A JSC is managed by a board of directors consisting of a minimum of three and a maximum of 11 members and shareholders are represented on the board in proportion to their percentage shareholding. As opposed to LLCs where managers' statutory duties mainly involve disclosure obligations, in a JSC there are typically more stakeholders' interests involved and directors' duties are numerous. Such directors' duties can be classified under the broad categories of: (i) continuous disclosure, pursuant to which directors are obliged to disclose transactions involving conflict of interest; (ii) non-competition, pursuant to which directors are required to avoid getting involved in activities competing with the company's business; (iii) exercising good-faith, pursuant to which directors are required to exercise good faith in carrying out their duties; and (iv) maintaining confidentiality, pursuant to which directors are required to maintain the confidentiality of matters discussed in general assembly meetings.

Similar to managers in an LLC, the directors in a JSC are also generally liable for any loss suffered by the company or the shareholders or third parties as a result of their violation of the company's regulations or bylaws. The liability in this regard is applied jointly between all members of the board if the loss is a result of a decision taken unanimously. However, if the loss is a result of a decision that is passed by a majority, members of the board who have expressly rejected the resolution in the minutes of meeting shall not be held liable. Under the previous regime, the maximum penalty was a three month to a one year imprisonment and a fine of SAR 5000 to SAR 20,000 and this was imposed for various violations related to the disclosure and illegal distribution of profits, among other things. Under the new regulations the scope of potential liability and penalties for directors in JSCs has been expanded for certain violations.

Under the new regulations, the maximum penalty provided for directors in a JSC has substantially increased to become imprisonment for a term not exceeding five years and a fine not exceeding SAR 500,000 (or both) for various violations related to disclosure, abuse of authority or failing to convene a general assembly or shareholder meeting or not taking the necessary steps upon becoming aware that a company's losses have exceeded 50 percent of its paid-in capital.

Similar to the requirements of an LLC, if the losses of a JSC exceed 50 percent of the paid-in share capital at any time during the financial year, any officer or the auditor must inform the chairman who

must in turn inform the members of the board. The board must convene a general assembly meeting within 45 days of becoming aware of the losses to either increase or decrease the company's capital so that losses become less than 50 percent of the capital or liquidate the company.

Conclusion

While the new regulations have generally maintained the same basic thresholds for managers and directors duties and liabilities in LLCs and JSCs, they have increased the potential exposure to liability for managers and directors managing companies with increasing levels of loss.

The practical implications of the new liability threshold remain to be seen; however, while under the previous regime, individuals were willing to accept directorship positions and take on passive roles in management in return for remuneration, such an approach would now potentially expose the relevant individual to imprisonment and significant penalties as the standard of diligence for individuals managing companies, particularly those nearing distress, has increased. Also, while the recent amendments may be regarded as deterrents for management to take reasonable risks, they should instead be interpreted as an attempt by the Saudi legislator to promote active, efficient and effective decision making processes. Also, and in light of the above, we expect that Saudi Arabian insurance companies may be the biggest beneficiary under the new regulations through a rise in demand for D&O insurance from members of management and boards of companies in Saudi Arabia. R&C

Nabil Issa
Partner
King & Spalding LLP
T: +966 11 466 9409
E: nissa@kslaw.com

James Stull
Partner
King & Spalding LLP
T: +971 4 377 9929
E: jstull@kslaw.com

Sayf Shuqair
Associate
King & Spalding LLP
T: +966 11 466 9413
E: sshuqair@kslaw.com

MINI-ROUNDTABLE

CREATING OPPORTUNITIES USING BIG DATA AND ANALYTICS

PANEL EXPERTS

Jacob Gilden
Associate
Good Harbor Security Risk Management
T: +1 (202) 212 6680
E: jacob.gilden@goodharbor.net

Jacob Gilden is an associate at Good Harbor Security Risk Management where he advises executives and corporate boards on cyber security technology, the threat landscape and cyber risk management. Prior to joining Good Harbor, Mr Gilden took part in Lawrence Livermore National Lab's Cyber Defenders programme working on cyber security policy and congressional affairs. Mr Gilden holds a B.A. in International Relations from the University of Southern California and an M.A. in Government from Georgetown University.

Daniel Miessler
Director of Client Advisory Services
IOActive, Inc.
T: +1 (415) 254 3589
E: daniel.miessler@ioactive.com

Daniel Miessler specialises in creative problem solving that leverages an active 17-year technical background, a deep understanding of existing product and service solutions, and concise, transparent communication style that adjusts to any audience. Mr Miessler's previous experience includes web, mobile and network penetration testing, vulnerability assessment, audit, security architecture, risk assessment, firewall engineering, intrusion detection and prevention, and vulnerability management.

Eric Haller
Executive Vice President
Experian

Eric Haller is the executive vice-president of Experian's global DataLabs. He leads data labs in the US, UK & Brazil that support research & development initiatives across the Experian enterprise. Prior to Experian DataLabs, Mr Haller had responsibility for the management and growth of online credit profiles as well as strategic markets such as internet delivery, government, capital markets and retail banking for Consumer Information Services.

RC: Why is it important for companies to understand the growing importance of Big Data and analytics? What are the main factors driving the adoption of these processes?

Gilden: Big Data analytics are going to be increasingly incorporated into every type of business, whether for marketing, advertising, increasing productivity, driving business intelligence, security or consumer product offerings. The ability to harness and analyse data will increasingly become a differentiator across industry verticals. Big Data, as a business imperative, is driving companies to put in place better processes and technologies for collecting, storing and analysing data. Analytics will be the bedrock of the modern enterprise and applied to nearly every business challenge where quantitative data can be easily collected, stored and analysed. Big Data analytics as a competitive differentiator is driving adoption across enterprises.

Miessler: Big Data and analytics has everyone's attention because it offers the promise of significant and continuous business optimisation. There are thousands of potential optimisations to be made in any process, but humans are especially ill-equipped to identify and present these opportunities to businesses. Companies that implement Big Data and analytics can integrate these discoveries and optimisations into their standard operating procedures, allowing the business to function more efficiently as conditions change. This leads to reduced costs, maximising of opportunity and generally superior performance.

> **"The ability to harness and analyse data will increasingly become a differentiator across industry verticals."**
>
> *Jacob Gilden, Good Harbor Security Risk Management*

Haller: Data is at the centre of almost every product or process that exists in business today. Those that harness it for better risk management, marketing or operating efficiency can give themselves a competitive advantage and be more successful in their endeavours. Even industries that most would have thought were data irrelevant, like taxi cab driving, have become reinvented almost overnight by those that thought the process could

become much more efficient by creating a platform for data to be captured and analysed to eventually build a superior service offering. Competition inevitably drives change and in this case almost all businesses are under pressure to understand this data evolutionary progression.

RC: What opportunities does the ascendance of Big Data – both structured and unstructured – present to companies? Alongside the opportunities, how would you characterise the associated challenges that companies face when adopting it?

Miessler: The opportunities are identifying trends and patterns that would otherwise be missed, and then using those observations to readjust the business based on this new information. Human-run businesses tend to do this poorly, at long intervals, because it is so difficult to find truth in data without bias. Structured and unstructured learning allow one to continuously optimise in this way, giving the business a major advantage. Challenges include the integration of these technologies into business processes, and ensuring that the output of the algorithms is valid and that they should be used to adjust the business. In the early days, it will also be a challenge just to find the right products and services that are tailored specifically for your business.

Haller: One could write an encyclopaedia set on the opportunities with Big Data, so I would just say look at everything around you and ask yourself how it could be better. When you find something that makes your top three list, ask yourself what does better look like and what would you want to know to achieve it. I think you will find in most cases that where data and analytics becomes centre stage, the challenges are likely not what you might think. It is not the infrastructure – although finding somebody comfortable with architecting a Hadoop cluster is becoming a bit of a scarce resource these days because of such high demand. But assuming you can get past that hurdle, the high hurdles are around finding people with a solid understanding of the business you are trying to analyse through data and analytics, and data scientists who actually are proficient with the right skills to do the analysis. It is slow, inefficient and challenging to be successful when the people who know the business well are in a different part of the organisation than those who know data, analytics and solutions development. That happens frequently in big business.

Gilden: Big Data, if harnessed correctly, provides the potential to understand the intricacies of one's business like never before. Big Data analytics allows companies to find insights and opportunities that they may have missed previously and potential weaknesses in strategy. It will also offer enterprises the ability to better understand their customers

and their needs in order to tailor products and solutions. Security is one central challenge for Big Data. Companies are struggling to protect data that is centrally stored and managed. As the use of Big Data analytics grows, both the scale and scope of data stored will increase and analysis capabilities will proliferate throughout enterprises. Enclaves within enterprises will likely be using their own analytics solutions on their own stores of data making management and security monitoring a significant challenge.

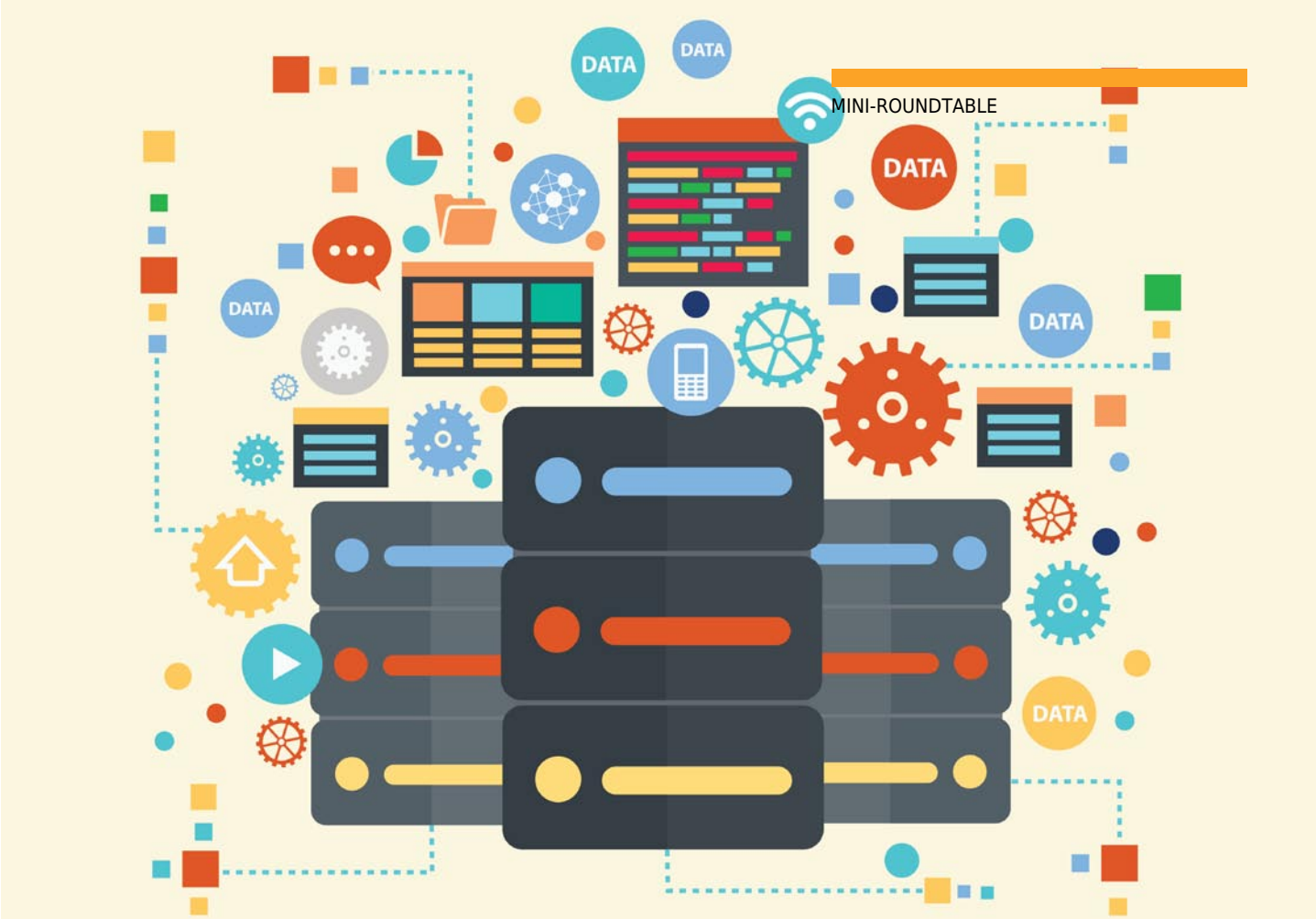
RC: Focusing on a few specific areas, in what ways can companies utilise Big Data and analytics to identify customer trends, build new revenue streams and detect potential fraud?

Gilden: Big Data analytics is a potential game changing technology for fraud detection. Payment card networks are investing heavily in Big Data analytics capabilities in order to better serve their customers and identify fraud in real time. Networks are collecting hundreds of different data attributes about individual payments, allowing them to analyse every transaction that is made in order to identify fraud. By creating a baseline of normal activity for a certain user, anomalous or potentially risky activity can be identified in real time, offering banks the opportunity to make risk-informed decisions about whether to cancel or authorise a payment and whether to notify a customer that their account information or card may have been compromised.

> **"One could write an encyclopaedia set on the opportunities with Big Data."**
>
> *Eric Haller, Experian*

Haller: One area of focus is detecting fraud, and many methods can be deployed using Big Data. Such methods range from analysing billions of transactions and leveraging deep learning to detect unusual spend behaviour patterns indicating fraud, to building an expansive network of identity data elements that are constantly analysed for changes in clusters that may indicate identity theft. Many machine learning techniques today are very well suited to detect anomalies that are often associated with fraud.

Miessler: One interesting way this will play out is in prediction of purchases. Monitoring Twitter, for



example, for tweets by people saying things like, "she said yes!", will be combined with what is known about that person. They live in Austin, TX. They went to UT. They studied finance. And so on. This will allow advertisers to specifically target them with what we already know their next purchases will be, when they will make them, and what types of products and services they will want. All this is made possible by Big Data and analysis, powered by machine learning.

RC: What advice can you offer to chief information officers (CIOs) on collecting and presenting data in a way that allows business leaders to understand and make critical strategic decisions faster than the competition?

Haller: CIOs should partner with their business colleagues, leverage their knowledge and couple them as tightly as possible with data scientists – if they have them.

Miessler: CIOs should talk about the patterns that are being shown by the algorithms and tie those patterns to stories. If we learn that people of this type, who go to this school, who date these types of people, who announce that they are getting married, tend to go on to purchase product A, product B and product C, then that is major. If you then go on to say that you recommend changing the product to better take advantage of this information, you are now talking about something tangible in the business. You are talking about the customer. You are talking about how they behave in the real world. And you are asking to adjust the business based on this. That is tangible. It is not about the tech; it is about what it tells us about the real world.

Gilden: Raw data or large macro figures are largely not useful for executives that need to make strategic decisions for the business. Presenting data graphically or through scoring can help business leaders understand the data they are looking at, how it will impact the business, and trends over time. If it is relevant for the area being examined, benchmarking against industry peers or competitors can also help executives understand the larger context of data and evaluate how the company is progressing. For example, an emerging class of cyber security companies are using data analytics to score the security of enterprises based on the traffic patterns emanating from their networks. These scores, while not perfect measures of security, can provide executives a snapshot of how the enterprise is doing vis-à-vis competitors and better understand key risks, specifically to and from critical vendors and partners.

RC: In this age of ever-growing data volumes, what strategies should companies deploy to mitigate the risks of being swamped by a data deluge as well as compromising sensitive information?

Miessler: Data security is critical, and it will soon be best practice to employ a corporate data lake that understands these risks and knows how to control authentication and access control. Many systems will need access to this data, and it is crucial that the access be granular and restricted in order to avoid disclosure issues. This is all on top of general cyber security hygiene that will become more important than ever.

Gilden: One of the challenges stemming from the emergence of Big Data is properly securing sensitive personal and corporate information that is being collected and analysed. Anonymising raw data as it is being stored can help reduce the risk that, if compromised, data can be easily traced to an individual in order to target them and helps protect the privacy of individuals. Anonymisation becomes much more difficult once data has been correlated and analysed as patterns derived can help link data

to individuals. Deploying encryption, whenever possible, is also important for reducing the risk of breaches. Encryption should already be a central part of any data security programme, but becomes even more important as companies collect greater amount of sensitive information about their own operations, which could be used for competitive gain, and about their customers.

Haller: There is a $1 trillion dollar commercial cloud computing market that is emerging to answer this very question. More companies are creating hosted analytic sandboxes that allow them to analyse large amounts of data in a safe, compliant environment using multiple data assets and sophisticated modelling and machine learning tools. This includes solutions that require quadrillions of calculations on billions of transactions.

RC: To what extent are social and economic changes likely to fuel the continued rise of Big Data and analytics? How should companies respond to these dynamics, and the opportunities they present?

Haller: Big Data only becomes truly powerful when it is compiled, sorted, analysed and manipulated – when it is translated into the language of business leaders and policymakers. And so the explosion of data has driven the emergence of fields built for the sole purpose of making data usable. Today, we see entire disciplines and areas of business that have been born of the need to glean insights from vast amounts of otherwise indecipherable information. In particular, the profession of the data scientists has emerged and must be embraced by organisations to meet this growing need – to bring structure to large quantities of formless data – so that we can do good things with data for our society and the economy.

> **"As markets become saturated with similar-sounding products, the quality of your product will become the quality of your algorithms."**
>
> *Daniel Miessler, IOActive, Inc.*

Miessler: One way this will have an impact is in increasingly competitive markets. As markets become saturated with similar-sounding products, the quality of your product will become the quality of your algorithms. The more you are able to anticipate customer needs and present them in compelling

ways, the better off your business will be in an environment of strong competition.

Gilden: Social movements could significantly impact the adoption of Big Data analytics and how companies use analytics technologies, especially if social initiatives translate to political action. Specifically, issues of privacy and the right of individuals not to have their personal information correlated or to control how their data is used is a major threat to the business model of many organisations that leverage data analytics. Just as the emerging 'right to be forgotten' has significantly impacted search engine and social media companies in Europe, a 'right to not be correlated' could significantly impact the use of Big Data analytics across industries. Big Data potentially threatens traditional notions of informed consent and privacy protections because individual pieces of information that by themselves may not threaten privacy, can provide a detailed picture of an individual when correlated and analysed. Changes in social understandings of privacy, especially in the United States where private companies currently face few restrictions on their collection of personal data, could threaten how companies leverage data and use analytics capabilities.

RC: What trends and developments do you expect to see in the Big Data and analytics space in the coming years?

Overall, do you believe the ability to collate data effectively and facilitate faster decision-making will be the key to a business remaining competitive?

Gilden: The ability to collect, analyse and use data is already a differentiator between successful and failing businesses and that trend will only continue and grow. While analytics will be an imperative for success on the client side of the business, and in many industries already is, I expect data analytics to grow significantly in the back office and in corporate management. In security, analytics are already being applied across the security stack to increase the efficacy of existing investments and lower the high burden that is placed on network security analysts. For a hard problem like cyber security that companies are not addressing well, analytics offers one of the best hopes for improved outcomes, lower costs and better metrics. They are not, as some are treating them, a panacea, however.

Haller: In terms of talent, exceptional analytic and software engineering talent is in very high demand. As a result, the responsibility to train high potential talent is falling on the universities and employers. Over the past three to five years, this balance has been almost entirely placed on the employer and we are seeing top tech companies hoard talent and even poach top professors in these fields to create

a competitive advantage for themselves. For most of us, we cannot hire a world scholar. So it is imperative for us to create programmes that develop people as they exit universities into data scientists. Over time, as we are already starting to see, the universities will catch up, students will exit requiring less training, and supply and demand will start seeing a bit more balance. But I believe we still may be five to ten years away from seeing this equilibrium take place. In terms of business acumen versus data science, the world of science and business are on a collision course. The old model was MBAs on one side of the company and engineers on the other. That model is busted; it is too slow and inefficient. Clearly, it still happens today but competition has a way of driving change. Scientists are more and more embracing the knowledge of business to improve upon what they are able to understand and innovate while product marketers are becoming more technically skilled. In many industries, we may find ourselves entering into an era where it will be hard to tell the two of them apart based on their education, skills or tasks.

Miessler: The biggest changes in the next few years will be products that integrate directly into business workflows. So a normal flow to execute a business transaction is A to B to C. But now it will include an additional step before C, where algorithms analyse all available data and determine whether the business should behave differently, provide a different experience, and so on. It will take time for businesses to come to trust such algorithmic recommendations, and not all recommendations will be of the same quality. But as the technologies improve, and become tailored to specific types of business, these integrations will become more common and more trusted over time. R&C

PERSPECTIVES

USING BASEL III PRINCIPLES FOR RISK DATA REPORTING TO IMPROVE DATA ANALYTICS

BY **EVA SWEET**
> ISACA

The Basel Committee on Banking Supervision developed the "principles for effective risk data aggregation and risk reporting" as part of its efforts to help Globally Significant Banks (GSBs) improve processes and controls to consolidate and report risk data at the entity level. The need to update the Basel framework and develop the principles originated from GSBs' inability to demonstrate accurate risk exposure during financial crisis of 2007-2008.

GSBs and other significant financial institutions were mandated to implement the necessary processes, systems and controls to meet compliance with the new Basel III framework (including the 14 principles) by 1 January 2014; however, new provisions are to be phased in between 2014 and 2019. In December 2011, the United States Federal Reserve announced that it would implement substantially all of the Basel III rules by 2016 at the earliest.

The main objective of the Basel III framework is to strengthen the regulation, supervision and risk management of the banking sector in the European Union. However, adoption of the 14 Basel principles for risk effective risk data aggregation and risk reporting can prove beneficial beyond risk reporting within the banking industry, because good quality data has the potential to benefit any organisation

using Big Data and data analytics to gain competitive advantage.

The 14 Basel principles for risk effective risk data aggregation and risk reporting can be grouped into four dimensions as follows: governance and architecture; data aggregation; reporting and supervisory review.

The 14 principles are: governance; data architecture and it infrastructure; accuracy and integrity; completeness; timeliness; adaptability; accuracy; comprehensiveness; clarity and usefulness; frequency; distribution; review; remedial actions and supervisory measures and home/host cooperation.

Using the 14 Basel Principles to improve data analytics

The foundation of accurate risk data aggregation and reporting is to have good quality data, which is directly related to having good metadata governance and management.

Metadata can be generated any time data is created, acquired, added, deleted or updated in any data repository or system included in the scope of a data governance and management programme. Metadata management can help improve data analytics capabilities because it helps organisations establish consistent definitions for business terms and establish consistent attributes to determine data origins.

Data analytics can help organisations make informed operational and strategic decisions that require accurate data and repeatable reporting procedures. In short, data analytics requires the same level of data integrity, uniformity and correctness mandated by the Basel framework.

Governance and architecture

To realise all the benefits of data analytics, organisations should implement a robust data governance framework, define and document the data architecture and also the IT infrastructure. These critical activities will help create the appropriate environment to meet the criteria established in the 14 Basel principles, which in turn will help develop data analytics capabilities.

> **"The foundation of accurate risk data aggregation and reporting is to have good quality data, which is directly related to having good metadata governance and management."**

This dimension contains only two of the 14 principles, however; this can be a very complex goal to achieve because to launch a data governance programme requires identifying all data sources, processes using data in scope, interfaces with internal and external parties and the business rules used to process data into meaningful information.

Implementing the first two principles should create outputs that enable the implementation of the remaining 12. Some of the most important outputs are outlined below.

Consistent glossary of terms. It is important to clarify terminology used within the same enterprise in preparation to use data analytics. For example, if one entity uses the term 'customer' while a different entity uses the term 'client', the data glossary will help reconcile both terms as meaning the same thing and any data analysis about sales will include customers and clients, thus presenting a more accurate picture.

Data lineage. Data governance depends on generating metadata containing information about the origins of data in scope. For example, data lineage includes attributes that indicate format, location, ownership, users, processes that use the data, data change timestamps and authorisation levels needed to process the data. In short, metadata allows the enterprise to visualise the data

lineage between the point where data originates through the point when data is reported.

Clear view into data architecture and IT infrastructure. Once the enterprise defines and documents the data architecture and IT infrastructure (in scope) it will be possible to create graphical representations of the technical environment. A visual representation can help identify gaps, dependencies and redundancies that must be addressed in order to create more efficient data flows.

Data aggregation

The principles in this dimension ensure accuracy, integrity, completeness, timeliness and adaptability, which are considered the attributes that increase value and reliability on information. Data aggregation principles require all possible sources of relevant data to be identified and associated in order to provide comprehensive reporting.

Data aggregation principles are critical for enterprises that have complex IT environments or dispersed operations. Using data aggregation principles can enable accurate and reliable data analysis because all relevant sources of data across the enterprise will be available.

Data aggregation relies on the outputs of the first dimension (consistent glossary of terms, data lineage, and data architecture and IT infrastructure documentation) and the controls (automated or manual) that ensure accuracy, integrity, completeness, timeliness and adaptability. It is safe to assume that data analysis relies on the same preconditions to generate reliable reports to help enterprises make educated decisions.

Reporting

Accurate, complete and timely data is the foundation of reporting, independent of the nature of the reports. However, reports must also be available at the right time and provide the context needed to make decisions.

Data analysis must yield accurate and comprehensive information presented in the appropriate context for the user making decisions based on the analysis reports. User needs and the purpose of the reports will determine the frequency for data analysis reporting and distribution. As mentioned earlier, data must be accurate and complete, but that is not enough. For data analysis to be valuable, reports must be available when the user needs them and in a context that is clear to understand.

Supervisory review

The last dimension of supervisory review is as critical as the first dimension of governance and architecture definition. The principles in this dimension ensure that data quality is sustained by conducting periodic reviews that either confirm compliance with all 14 principles or identify

weaknesses that must be addressed in order to restore compliance.

To sustain the value created through data analysis, data quality must be sustained. New processes or applications that are added, modified or decommissioned can impact the quality of the data pool used for data analysis, thus implementing the principles in the last dimension is critical to continuing the generation of reports that are accurate and reliable.

Conclusion

The Basel Committee developed a framework intended to help large banks with their risk reporting capabilities. However, the adoption of the 14 principles for effective risk data aggregation and risk reporting can benefit any organisation that wishes to use Big Data and data analytics because data analytics depends on data quality and data quality depends on data governance and good data management practices.

Data governance can help enterprises achieve data integrity, uniformity, completeness and accuracy. The first step to implement a data governance programme is to define what metadata should be generated, define the data architecture, define the IT infrastructure and identify all sources of relevant data.

The next steps consist of implementing controls that ensure accuracy, integrity, completeness, timeliness, adaptability, comprehensiveness, availability and context. At this point, the enterprise can start relying on data analysis reporting to make decisions and start the next steps to ensuring data quality sustainability. R&C

Eva Sweet
Technical Research Manager
ISACA
T: +1 (847) 660 5581
E: esweet@isaca.org

PERSPECTIVES

HOW TO MAKE SURE DATA SOLVES RISK RATHER THAN BECOMES A RISK

BY **TIM BARBER**
> PITNEY BOWES

Figures from the Office of National Statistics suggest that fraud is endemic. In the UK alone, almost six million fraud and cyber crimes – such as account hacking or identity theft – were committed in 2015, revealing that fraud is the most common kind of crime in the UK today.

Bank and credit account fraud in particular were cited as the most common, and widespread access to connected devices is exacerbating the problem: there were two million computer misuse incidents reported in 2015, including 'unauthorised access to personal information' and crimes involving a computer or device being infected with a virus.

In the corporate landscape, corruption and anti-money laundering (AML) are high on the global agenda, more so than ever in today's digital borderless world of commerce. Despite tighter regulations and record penalties for non-compliance, as well as deeper media scrutiny and a drive toward transparency across the public and private sectors, corporate fraud is widespread with more than 36 percent of organisations experiencing economic crime in the past two years.

There is now a very clear need for countries to become bullish and more vocal in their approach to eliminating systemic fraud. Governments are responding to this need by bringing in a series of far-reaching changes designed to stamp out corruption, money laundering and tax evasion across the

corporate landscape, and in doing so aiming to minimise this major risk for businesses.

Measures proposed in the UK government's Criminal Services Bill, for example, will reach far deeper than the current requirement of businesses to prevent bribery and tax evasion. The most significant change for UK businesses under the new crackdown is that failing to prevent money laundering inside businesses will become a new corporate offence. And if an employee is charged with money laundering offences and fraud, the business will be held liable unless it can demonstrate it had preventative procedures in place. When the bill becomes law, businesses will not just face regulatory penalties – they will face legal proceedings.

But in spite of these proposed regulatory changes and the huge potential impact of fraud on a business, there is a worrying, and surprising, level of apathy across many organisations. PwC compared the results of its 2016 Global Economic survey with findings in its 19th Annual Global SEO survey. The result was concerning: where two-thirds of chief executives felt there were more threats to the growth of their companies than ever before, one in five businesses had not carried out a single fraud risk assessment in the last two years. Their research also reveals that one in 10 economic crimes are uncovered by chance.

Businesses can no longer afford to leave economic crime to chance: the risks are far too high, with the impact potentially catastrophic on an organisation's reputation, performance and future. Knowing who their organisation is doing business with is the key, and is probably the single most powerful capability a business has in its fraud prevention armoury. Inaccurate, unstructured data stored in multiple

locations, accessed from various devices by different people, and without robust protection, is a major threat to a business, leaving it exposed and vulnerable. Businesses have an obligation to themselves and their clients to protect their data and to fill any intelligence gaps.

Conversely, accurate, detailed, current data organised in a consistent, transparent way is an asset, a key to compliance, and a means of eliminating risk. Organisations need to have software and systems in place which ring-fence and link data, taking it from multiple sources across a business and determining whether it refers to the same individual, asset or location. This drives compliance and ensures clean, structured data.

Crucially, the data must be accessible quickly and securely so businesses can ensure their customer due diligence (CDD) is fast, thorough and accurate. This is hugely important for businesses – retailers in particular – at the moment, as the European Fourth Anti Money Laundering Directive now requires CDD for anyone trading goods in cash with a value of more than €10,000. Prior to June this year, the figure stood at €15,000, so background checks will increase in number, resulting in frustrating delays for customers, a decrease in high end sales, and a potential impact on reputation.

The directive also requires changes to rules applying to Politically Exposed Persons (PEPs). A PEP is defined by the Financial Action Task Force (FATF) as "an individual who has been entrusted with a prominent public function". PEPs present additional risks to a business, as the FATF recognises that the very nature of their positions exposes them to abuse for the purpose of committing fraudulent offences such as money laundering, corruption and bribery. The increased risks PEPs bring require an organisation to apply additional measures to prevent such crimes and to detect such activity.

> **"Businesses have an obligation to themselves and their clients to protect their data and to fill any intelligence gaps."**

Under the new directive, local PEPs are subject to the same rules as overseas PEPs. This means that UK officials with prominent public functions, and potentially some of their relatives and close associates. And the conversation on PEPs is set to continue, as the new Bank of England and Financial Services Act 2016 requires the FCA to provide

guidance on the definition of a Politically Exposed Person.

It is becoming even more important for an organisation to know exactly who it is doing business with; who they in turn are doing business with; how they obtain their assets; and what they do with those assets. The ability to extract meaningful insight from an organisation's data is very powerful in reducing risk, as certain software and applications enable businesses to quickly find, link and visualise complex relationships across parties, accounts and transactions.

For those organisations struggling with a consistent global approach to their data management – integrating disparate systems after M&A activity, for example – intelligent software has capabilities to localise and standardise names. 'Michael' may be known as 'Michel' in France, or 'Mikhael' in Eastern European countries, for example.

Each entity doing business with the organisation can be assigned its own unique identification number, and data from multiple sources can then be appended to this specific entity, improving insight and accuracy. This level of precision helps to reduce false positives and false negatives, limiting time and costs spent on manual checks and ultimately improves the customer experience.

Data should minimise risk, not become a risk, but for many organisations it adds to the complexity of compliance. As regulators and governments continue to crack down on financial crime across our global economy, the responsibility falls on businesses to protect themselves, their customers, their employees and stakeholders – or pay the price. R&C

Tim Barber
Director, Software Solutions
Pitney Bowes
T: +44 (0)1491 416 600
E: tim.barber@pb.com

PERSPECTIVES

THE NEW PRIVACY SHIELD FINALLY ADOPTED – BUT THE PROBLEMS MIGHT NOT BE SOLVED

BY **ELSEBETH AAES-JØRGENSEN, JENS HARKOV HANSEN AND STINA LINDBERG HANSEN**
> NORRBOM VINDING

The EU-US data transfer framework known as Safe Harbor was declared invalid by the European Court of Justice (ECJ) on 6 October 2015 in the *Schrems* ruling. Now, the European Commission has adopted a new regime, known as the EU-US Privacy Shield, to address the concerns raised by the ECJ when it struck down Safe Harbor. Based on the new regime, companies will be able to transfer personal data across the Atlantic – including data on employees and customers.

The legal background

The legal background for the new Privacy Shield is the EU Data Protection Directive. According to the Directive, a specific legal basis is required to transfer personal data to a third country, regardless of the nature of the personal data. This will also be the case when the Directive is replaced by the General Data Protection Regulation (GDPR) in 2018, as the GDPR contains similar requirements.

Under the Directive (and the GDPR), various instruments are accepted as legal basis for transferring personal data to a third country. The most common instrument is entering into an agreement implementing what is known as 'EU Model Clauses' (standard EU approved terms for data transfer). However, in relation to transferring personal data to the US, another common instrument was signing up to the 'Safe Harbor'; a framework approved by the Commission and operated by the US Department of Commerce. Companies in the US that had joined the Safe Harbor framework were regarded as ensuring "an adequate level of protection" for personal data, allowing personal data from the EU to be transferred to such companies.

"A specific legal basis is required to transfer personal data to a third country (i.e., a country outside the EU or EEA), regardless of the nature of the personal data."

Snowden, Schrems and Facebook

The decision to declare the Safe Harbor framework invalid was based on the repercussions of Edward Snowden's leaks. Based on these, the Austrian Facebook user, Maximillian Schrems, decided to challenge the Safe Harbor framework. He complained to the Irish Data Protection Commissioner, stating that Facebook transferred personal data to a server in the United States allowing the US authorities to access his data. His complaint was rejected by the Irish Data Protection Commissioner and the case ended up before the Irish courts. They decided to request a preliminary ruling on the question from the ECJ.

The ECJ was asked to address the question of whether the Irish Data Protection Commissioner was prevented from investigating the complaint due to the nature of the agreement between the EU and the US making the Safe Harbor framework possible. As part of the agreement, the Commission had decided that US companies – under the Safe Harbor framework – ensured an adequate level of protection for personal data transferred to the US. But because Mr Schrems and the Irish courts expressed doubts on the validity on the Commission's decision making the Safe Harbor framework possible, the ECJ took a direct position on this question.

On 6 October 2015, the ECJ ruled that the Commission's decision on Safe Harbor was invalid. The ECJ found that the decision did not meet the

requirements in the Directive and, accordingly, did not ensure an adequate level of protection. Furthermore, the ECJ ruled that the Commission had exceeded its powers by limiting the national data supervisory powers to investigate the level of protection in the US.

Based on the ECJ's ruling, the transfer of personal data under the Safe Harbor framework was suspended.

The new Privacy Shield regime

The ECJ's ruling was groundbreaking because it gave rise to considerations as to whether transfer of personal data to the US would be possible at all. After the ruling, negotiations were initiated between the EU and the US to find a new common sustainable solution that would allow the lawful transfer of personal data to the US. In February 2016, the Commission published a draft agreement to be entered into between the EU and the US – the so-called EU-US Privacy Shield Agreement. The purpose of the Agreement is to find a new basis for the transfer of personal data to companies in the US in the post-*Schrems* era.

After negotiations and a series of improvements to the draft – e.g., based on criticism from the body of EU regulators known as the Article 29 Working Party (Working Party) and in light of the *Schrems* ruling – the Commission decided on 12 July 2016 that the new Agreement ensures an adequate level of protection for the transfer of personal data to the US.

Compared to the former Safe Harbor framework the new Privacy Shield regime contains a number of stronger safeguards. Thus, the overall purpose of the new regime is to ensure and

protect Europeans' right to privacy by protecting their personal data. To obtain the protection intended, US companies must commit to a set of Privacy Shield principles.

The Privacy Shield principles provide new, stricter and stronger obligations for US companies in regard to handling and storing of personal data. This is reflected by the principle on notice and information to individuals. This principle ensures that the data subjects receive information on the purpose of the collection of their personal data. Further, the data subjects are ensured access to their own personal data making it possible to amend, correct or delete inaccurate information. Also, the new principles on security, data integrity and purpose limitation, recourse, enforcement and liability are intended to impose stronger obligations on US companies under the Privacy Shield regime.

Moreover, US companies will be subject to monitoring to ensure that they comply with the rules under the new Privacy Shield regime. Further, US companies must display their privacy policy on their website and in case of a complaint, they must respond expeditiously.

In addition, the new Privacy Shield regime addresses mass surveillance and US public authorities' access to personal data. Also, the Privacy Shield introduces an independent Ombudsperson mechanism. In order to achieve effective protection of Europeans' individual rights, the data subjects are given access to various remedies in case of a complaint. The Commission will in this context work out a short guide on what remedies are available for data subjects.

As of 1 August 2016, US companies that meet the criteria set up in the new Privacy Shield regime are able to self-certify and register with the US Department of Commerce for the so-called 'Privacy Shield list'. Companies must renew their registration annually.

Based on the new regime, companies will be able to transfer personal data across the Atlantic – including data on employees and costumers – and the new regime will thus be a suitable alternative to, for instance, EU Model Clauses.

The Privacy Shield might not solve the problems

Even though a new regime has been adopted, it may still be questioned whether the Privacy Shield actually addresses the criticism set out by the ECJ in the *Schrems* case.

The Working Party has recently – and after the adoption of the new regime – released a statement showing that some of their concerns still remain and indicating that the first annual review of the new regime will be a key moment to test the robustness of the Privacy Shield. For example, the Working Party is concerned about the independence and powers of the Ombudsperson mechanism. Further, the Working Party regrets the lack of concrete assurances making

sure that bulk collection of personal data does not take place.

The Working Party also announced that it will provide guidance on the application of the Privacy Shield and that alternative transfer tools can still be used but may be affected by the outcome of the annual review.

Thus, based on the above, the mechanism used for transferring personal data to the US might (again) be brought before the ECJ in a potential new *Schrems* case. And as the new general data protection rules – the GDPR – contain similar requirements on the transfer of personal data to third countries as under the current Directive, simply waiting for the new set of rules to enter into effect would not solve the problems. R&C

Elsebeth Aaes-Jørgensen
Partner
Norrbom Vinding
T: +45 35 25 39 79
E: eaj@norrbomvinding.com

Jens Harkov Hansen
Senior Associate
Norrbom Vinding
T: +45 35 25 09 41
E: jhh@norrbomvinding.com

Stina Lindberg Hansen
Junior Associate
Norrbom Vinding
T: +45 35 25 39 43
E: slh@norrbomvinding.com

PERSPECTIVES

EMBRACE THE ANALOGUE IN YOUR DIGITAL SUPPLY CHAINS

BY **DAVID NOBLE**
> CHARTERED INSTITUTE OF PROCUREMENT & SUPPLY

It is no secret that the internet has transformed supply chains. Whether it's metadata on the sell-by date of a cargo, real-time shipping progress or factories which know when they are running low on raw materials, modern supply chains now exist in both the physical and digital worlds.

In the rush to unlock the potential of these digital supply chains, however, we have opened up our businesses, organisations and economies to novel forms of fraud and theft by cyber criminals. As supply chain professionals we must adapt to these threats by investing in new skills and processes in the digital age. However, the most important skills for combating cyber crime may well still be routed in the analogue world.

A digital supply chain still encompasses all the elements of a traditional supply chain. Raw materials move from country to country across the value chain toward the consumer. Yet, while the factories, people and products which make up global supply chains can only move as quickly as the physical world allows, the digital supply chain allows them to communicate with each other instantaneously.

Indeed, some parts of our supply chain cease to exist in the physical world entirely. CDs, VHS tapes, maps, even children's toys have all been replaced to varying degrees by digital media, satellite navigation and online games. This shift from boxes to bytes allows products and services to move directly between their creators and consumers.

Whether we are concerned with this digital layer on top of traditional, physical supply chains or entirely new digital products, the world has benefited greatly from the digitisation of supply chains. The instantaneous flow of data allows the flow of raw materials to be sped up or slowed down automatically, responding to demand and output to keep costs down and meet the ever-changing needs of consumers and business. With faster, more accurate tracking, digital supply chains can respond quickly to logistical challenges, pricing changes or environmental crises.

But these benefits come at a cost. A recent study carried out by the UK government found that almost three quarters (74 percent) of small businesses, and 90 percent of large organisations had experienced

an information security breach in the course of a year. Severe security breaches cost large UK businesses an average of £1.46m with even SMEs losing £310,800 due to breaches.

This is because data travelling along the supply chain from start to finish can be stolen or even altered at various stages and just like physical supply chains, digital supply chains are only as robust as their weakest components. Perhaps the most famous cyber attack on a digital supply chain in the world is Stuxnet. This virus was allegedly created to sabotage Iranian nuclear centrifuges. Like many modern production facilities, the centrifuges rely on digital infrastructure to operate efficiently, an infrastructure which Stuxnet hijacked to force malfunctions and a break down.

The plants were theoretically immune from cyber attacks and cut off entirely from the internet. The weak link is thought to have been human error, with workers unwittingly delivering the virus in through the front door with 'infected' USB sticks.

Human errors such as this are not confined to large scale espionage; it is the weak link in many digital supply chains. Indeed, according to the UK government, the single most common cause for data security breaches in the country is avoidable human error.

So what can supply chain managers do to protect their supply chains against cyber security threats? First and foremost, it is vital to invest in new digital skills. The UK government's Cyber Essentials Scheme seeks to help businesses develop a basic understanding of data security and implement the five key controls: implementing firewalls, configuring networks appropriately, limiting access to the right people, installing malware and virus protection and ensuring security patches are swiftly installed.

"The world has benefited greatly from the digitisation of supply chains. But these benefits come at a cost."

But while the cyber security arms race shows no signs of slowing, it is increasingly important for supply chain managers to embrace the analogue 'soft skills' which can help businesses to detect when something is awry more quickly. The data at work across the digital supply chain is only as reliable as the people who manage, manipulate and understand it.

Just as any good supply chain manager will seek to understand the production facilities their suppliers use, they must also scrutinise the data protection processes and practices they employ. Furthermore, responding to a breach in the digital supply chain requires a coordinated response across the chain. This is only possible if these licensed professionals develop trust with their partners. This means knowing the individuals up and down the supply chain by name, speaking to them regularly and developing a shared resilience strategy. When the digital supply chain breaks down it is analogue networks which will ultimately take the strain.

The supply chain management profession is acutely aware of the tension between efficiency and resilience. Digital supply chains are no exception. The great benefits they promise also come with new, difficult to grasp risks. Ironically, the greatest tool in our armoury to mitigate these risks may be the human relationships we can so easily neglect. R&C

David Noble
Group Chief Executive Officer
Chartered Institute of Procurement & Supply (CIPS)
T: +44 (0)1780 756 777
E: press@cips.org

PERSPECTIVES

AN EXAMINATION OF THE GROWING TREND IN EMPLOYING EX-HACKERS FOR SECURITY PURPOSES

BY **MIKE GILLESPIE**
> ADVENT IM LTD

KPMG first commented on the growing trend for employing ex-hackers as part of cyber security regimes in business, back in 2014. A recent Radware survey indicated that only 18 percent of respondents did not employ ex-hackers. It seems hard to believe, but 46 percent reported they had had them in place for more than two years and 36 percent said they had installed them in their firms within the preceding two years.

Although the survey would benefit from a larger sample size, if we accept that there is a growing number of businesses that have installed or are installing ex-hackers, we can go on to ask, is this genuinely the future?

Looking at business culture, you would be forgiven for thinking that many organisations deal with security at arm's length, trying to solve problems or mitigate risk through buying software and passing responsibility onto single silos, such as IT. Anyone who understands our interconnected world will realise that this is not a sustainable approach.

Is employing ex-hackers another step on this cultural disconnect and wilful 'hands-off' approach? Not all organisations are structured this way, and not all will have taken the step lightly or without

significant exploration of the possible outcomes. Some, however, will embrace this regardless and potentially without a vital risk assessment and inclusion on the corporate risk register.

In this article we discuss some of the areas of potential concern for businesses considering this as a security solution. It is easy to see the attraction of having an ex-hacker on board, but would you be so quick to hire a convicted money launderer as a compliance manager?

Vetting as part of a recruitment process and ongoing pastoral care of employees will play a part in most employee lives. When it comes to recruiting an ex-hacker, the traditional vetting will potentially place an immediate roadblock on this solution. Given that most hackers gain their reputation by hacking systems illegally, it is very possible they will have a criminal conviction for this kind of behaviour. So, an exception would have to be made, along with a commitment to extensive pastoral care and monitoring.

The potential for friction with other employees is possible as the standard checks they are expected to pass in order to be employed are potentially waived for the ex-hacker; employees would not need to be privy to any personal information to be able to work this out for themselves. A business will end up using its own judgement about employing this person. Someone senior would need to be accountable for this decision as well as for the person themselves.

If you ever doubt how important this element is, remember that Edward Snowden showed many signs that were ignored, prior to his legendary data theft. Regardless of your position on Snowden, if you are not on top of your employees' pastoral wellbeing, you will pay the price – and this goes double for hackers. While they clearly bring something to the table, how much confidence do you have in that individual's trustworthiness long term? Are they a gun for hire, where the potential for reward outweighs what you are giving them?

Understanding the motivations of hackers is important if you are considering this route. On one hand, we are in a widely acknowledged skills gap in cyber security, which might lead one, not unreasonably, to assume that the financial aspect would be the paramount consideration for an ex-hacker who is prepared to go corporate.

They may be seeking the highest payday, and if you cease to match the continuing expectation, you could be left in the lurch if they take their skills elsewhere. Another consideration might be if they could be coerced by an outsider to steal, change or devalue information assets in an industrial espionage type of activity. They may also just decide to sell your assets to the highest bidder.

Again, this is if financial gain is their primary motive. With hackers this is not always the case and business needs to understand this. Many hackers have been in it either for laughs or for the kudos

"It is easy to see the attraction of having an ex-hacker on board, but would you be so quick to hire a convicted money launderer as a compliance manager?"

and reputation it brings them in their community. Sometimes, it isn't even as obvious as status.

If we were to use the main character in the hit TV series, Mr. Robot, he establishes from episode one that he is not interested in money. For him it is curiosity, challenge and a kind of moral code you only find with anti-heroes. This is hugely complex, and while need may drive an ex-hacker to seek employment, if you do not know the range of their motivations, you could come into conflict.

It is also worth mentioning that hackers are sometimes ideologically motivated. This may be harder to spot and you need to make sure that this is not going to be an area of either discomfort or

risk for either of you. By nature, ideological hackers do not tend to sit idly by if there is something they do not agree with, so be prepared for that. Understanding your business's core values and understanding theirs, combined with good pastoral care, could help.

By taking this route, we are effectively hoping for the best and side-stepping the risk, crossing our fingers that it won't backfire. We will probably never know how successful or unsuccessful this has been for the businesses that have trodden this route, as they may well be reluctant to talk about it. It will be interesting to see what impact, if any, it has on monetary penalties in case of any data breach involving these employees or what effect it might have on an organisation's cyber security insurance payout. Insurers may balk at a payout involving an ex-hacker if they think a business has basically handed the keys to their strongroom to a criminal.

On a positive note, if you have employed a successful hacker you know you have someone highly skilled, so the key then is to keep them happy, loyal and motivated. Make sure they are tied in to your core values if possible as they might not share them, but you have to accept that as part of the risk.

Other teams and departments need to understand what you have brought into the business. A business has a commitment to look after staff, but when you have someone who is a potential risk to the entire operation, you need to be even more hands on with pastoral care, early warnings and indicators, as by definition you have to give them privileged user status. Be clear with them about what their remit is and don't allow them to use your network to carry out other activities possibly unconnected to your business.

If the risk assessment is done and the risk owners have accepted the risk and agreed it is within the company's risk appetite, then you can proceed with a degree of confidence or at least full knowledge. But if a department is taking matters into their own hands by doing this autonomously, that is clearly a very different matter. It looks like hiring hackers is here to stay, for a while at least. R&C

Mike Gillespie
Managing Director
Advent IM Ltd
T: +44 (0)121 559 6699
E: bestpractice@advent-im.co.uk

MINI-ROUNDTABLE

TRANSACTIONAL INSURANCE

PANEL EXPERTS

Jeffrey Cowhey
President
Ambridge Partners LLC
T: +1 (212) 871 5402
E: jcowhey@ambridgepartners.com

Jeffrey D. Cowhey is co-founder and president of Ambridge Partners LLC. Mr Cowhey's professional experience includes service at Aon Financial Services Group where he served as executive vice president and member of the Executive Committee with management oversight of the East Coast region, and National Union Fire Insurance Company where he served as vice president of the Commercial Management Liability Division. He received a B.S. from LaSalle College.

Steven R. DeLott
Senior Counsel
Simpson Thacher & Bartlett LLP
T: +1 212 455 3426
E: sdelott@stblaw.com

Steven R. DeLott is senior insurance counsel and a member of the firm's Corporate Department. His areas of concentration include directors' and officers' liability insurance, representations and warranties insurance and insurance regulatory matters. Mr DeLott is a former adjunct assistant professor at the College of Insurance in New York City where he taught courses in insurance law and insurance regulation. He is also a member of the American Bar Association, Section of Tort and Insurance Practice, where he serves on the Public Regulation of Insurance Law Committee.

Brian Hendry
Head of M&A
Paragon International Insurance Brokers Ltd
T: +44 (0)20 7280 8276
E: bhendry@paragonbrokers.com

Brian Hendry has been head of M&A insurance at Paragon International Insurance Brokers since July 2014. He is a career insurance broker having joined the Transaction Liability Unit of Aon London in the late 90s from where he moved to Willis in early 2000 and led their Transaction Services practice for over 10 years. Mr Hendry has been closely involved in the evolution of the M&A insurance market and provides his clients with industry leading advice, innovation and insurance products.

Deborah McBrearty
Head of Transaction Risk Insurance
Tokio Marine HCC
T: +34 93 530 7393
E: dmcbrearty@tmhcc.com

Deborah McBrearty is a dual qualified (UK/NZ) solicitor who holds over 20 years' experience in private practice and the insurance industry. Since 2000, she has specialised in the Transaction Risk Insurance (TRI) field and is recognised as one the few professionals involved in this line of insurance since its infancy in the London insurance market. Her experience includes both broking and underwriting bespoke insurance solutions for M&A including: warranty & indemnity, tax indemnity, and prospectus liability products, among other forms of contingent risk transfer.

RC: Based on your experience, how would you describe current attitudes toward transactional insurance? To what extent are you seeing broader adoption of transactional insurance in today's M&A market? Are there particular types of transactions – by size or industry, for example – that are particularly well-suited to the use of transactional insurance?

Hendry: There are a number of key underwriting centres for transactional insurance that have evolved semi-independently as the products have been increasingly taken up. The more mature centres in UK, Nordics and Australia have seen consistent growth in the use of the product for over five years as M&A professionals experience the positive aspects of the products. The US market has grown phenomenally over the past 24 months and this acceptance in the US is leading to a greater understanding and adoption of the insurance across the globe. Based on the data we have collected, we consider that the take up of the products has grown by 20 percent year on year since 2008. The number of insurers offering M&A insurance has expanded rapidly over the past 36 months. Currently there are 28 insurers and we know of others that are due to launch shortly. As the transactional insurance market matures and develops, we expect that insurers will increasingly differentiate their offering by specialising on a sector basis, by geography, by size of transaction or by including coverage enhancements.

McBrearty: Awareness regarding warranty & indemnity insurance (W&I) – or representations & warranties (R&W) insurance, as it is know in North America – has grown dramatically over the past five years, with take up across Europe, US, Australia and New Zealand and more recently in Asia too. In southern Europe, in particular, where just three years ago this product was hardly known, it is now used regularly in some industries – for example, the real estate sector has notably widened its embrace of the product. As clients become more aware of W&I and its utility, their approach on how to employ the product becomes more sophisticated. We see it being used in the early stages of a negotiation, where sellers consider introducing the idea of its use in their offer on day one at auction. It is also not unusual to see a pre-negotiated insurance policy, in some jurisdictions, Australia, UK, Nordic countries, for example, being stapled to the first draft of the sales and purchase agreement (SPA) in the data room; just as you would for the financing of the transaction. In the beginning, its development sparked thanks to the private equity industry. Nowadays, the real estate industry and strategic buyers or sellers are also inclined to use W&I as part of their negotiation 'tool box' when they embark on M&A transactions.

Cowhey: Transactional insurance has grown from a relatively new niche insurance solution to a broadly accepted tool used to help transaction professionals bring a transaction to close. Transactional insurance, once considered only in the context of an M&A transaction, is now frequently used to help facilitate a broad array of transactions, including deals involving private equity, real estate, bankruptcy, refinancing and others. Broadly, most professionally structured and well diligenced business transactions can be considered candidates for the use of transactional insurance.

DeLott: I would describe current attitudes as being much more positive than in years past. Clients are increasingly accepting of transactional insurance as part of the deal. After an initial scepticism over whether introducing transactional insurance would slow down a deal and over how readily claims would be paid, many clients have become comfortable with the product. The policy forms have also become more favourable in recent years, with fewer standard exclusions. I am seeing transactional insurance being used in a wide swath of mid-market deals, across a variety of industries.

RC: Could you outline the key benefits of using transactional insurance as part of an M&A risk management strategy?

Cowhey: While the motivation for use of transactional insurance can vary from a prospective buyer's desire to strategically enhance its bid proposal, to a seller looking for a means to minimise its post-closing indemnification obligation, the essential and common benefit of transactional insurance is the ability to attract insurers to provide financially sound capital in support of enhancing, supplementing or replacing a part or all of the seller's indemnification obligation. This service can help the parties facilitate a more timely execution of a transaction while enabling the buyer to focus on management and integration of its newly acquired asset. Additionally, the seller can add a measure of certainty regarding the duration, scope and quantum of its post-closing indemnity obligations.

> **"I would describe current attitudes as being much more positive than in years past. Clients are increasingly accepting of transactional insurance as part of the deal."**
>
> *Steven R. DeLott,*
> *Simpson Thacher & Bartlett LLP*

DeLott: It seems to me that the principal benefit of transactional insurance to a risk management strategy is the likelihood that claims will be fairly and timely paid. Whereas a seller may have little incentive to pay indemnity claims quickly, the insurance carriers recognise that a reputation for favourable claims handling is necessary for transactional insurance to exist. Transactional insurance is not required in order to do deals. If the claims process is thought to be difficult, the market for transactional insurance would likely evaporate.

Hendry: Transactional insurance provides an efficient means to secure the amount and period of liability available for the contingent risks associated with M&A transactions. For financial sellers, a core factor is the ability to exit the investment 'cleanly', with minimal residual liability and therefore, distribute the majority of the consideration immediately following closing. For management sellers, in a secondary transaction, the exposure from breaches of warranties can be 'minimised' which allows for the re-investment into the target business to be safeguarded and in the event of an unknown issue, the business is not additionally impacted by loss of management focus. For buyers, they receive direct access to a liability package tailored to their specific requirements and from an insurer with a strong security rating. Furthermore, the cost of insurance can be absorbed within the overall transaction arrangement allowing the risk management strategy to be controlled from the outset of the process.

McBrearty: Traditionally, W&I has been used as an alternative for sellers to secure the transaction. The idea of not having to block money in an escrow account, securing a bank or mother company guarantee, as well as the insurance also offering a way of providing collateral to their obligations, being key benefits. Another benefit is that passive sales parties in the deal can obtain effective protection. The product has evolved in such a way that it is now more widely purchased by the buyer. In fact, roughly 85 percent of deals are being underwritten for the buyer-side. The buyer's insurance offers the possibility for the seller to limit liabilities as far as possible; limiting obligations under the SPA, offering a low seller's cap and/or limiting the period of indemnity. So it not only offers protection and a large degree of comfort – knowing that you can find recourse via the insurance policy – to the buyer, it also makes their bid more attractive.

RC: What types of transactional insurance products are currently available? How can such products assist in facilitating the successful completion of a deal?

DeLott: Although I have seen tax insurance on a few deals, the vast majority of transactional

insurance that I see is W&I insurance, usually purchased by the buyer, although at times by the seller. It is particularly useful where the seller is a private equity firm and would like to pay out all of the proceeds of the transaction to investors without having to wait for an indemnity period to expire. Corporate sellers have also found that to be desirable. In many auction situations, the sellers are requiring that the buyer obtain W&I insurance as the exclusive source of indemnity for a breach.

McBrearty: The traditional objective of a W&I policy is to cover all representations and warranties in a contractual document such as a sale & purchase agreement, in a fair and thorough negotiation and disclosure process. It insures financial loss arising from breach of these warranties and insures unknown issues. Tax indemnity insurance or 'tax opinion' is an effective risk transfer solution relating to any tax uncertainty surrounding a corporate transaction, such as M&A, investment or other. It covers the potential liabilities should the tax treatment employed be challenged by the relevant authorities. Contingent tax exposure may hinder the deal itself, and as such this insurance product acts as a deal facilitator. Any other potential and known risks in the transaction, investment or other, unrelated to tax ramifications or the relevant contractual documentation, also represent factors that may threaten the deal. Contingent risk transfer insurance offers a further risk transfer solution, bridging the gap between deal parties, and again acting as a deal facilitator.

Cowhey: While many transaction professionals think of W&I insurance, in connection with transactional insurance needs, such as buying or selling targets and private equity investment, transactional insurance also includes tax insurance, contingency insurance and other niche solution products. Like W&I, tax insurance and contingency insurance can help facilitate a transaction by which an insurer provides a 'ring-fence' around potential costs associated with the unintended consequence of an adverse determination by a tax authority on a specific and covered tax issue. This insurance can allow the parties to proceed with negotiation and diligence when a particular tax issue might otherwise bog down the parties in protracted discussions regarding potentially applicable administrative agency guidance, case law and quantum of damages.

Hendry: W&I is by far the most utilised of the products, with tax opinion insurance and contingent risk insurance also regularly arranged. The core objective is to transfer transaction liability risks related to the target from the balance sheet of a seller or buyer to an insurer. W&I insurance is designed to cover unknown issues, whereas tax opinion and contingent risk policies insure issues that have been identified during the transaction

– normally with a profile of high severity, low probability.

RC: Could you provide an insight into how pricing and terms for transactional insurance have evolved in recent years to meet market demands? How do the pricing and terms for transactional insurance differ between the US and the UK?

McBrearty: In 2010 in Europe and Australia, average cost was in the range of 2-4 percent of the limit purchased, rate on line (ROL). These days, the premiums have become more competitive – there are more entrants to market and thus more available capacity. The average ROL, depending on the jurisdiction, is in the region of 1-2 percent with further discounts applying to some industries considered to be less risky, such as real estate, for example. Retention schemes have also evolved from the typical 1-2 percent of the equity value to now more sophisticated retention schemes from 0.5-1 percent for straightforward deals. The market is also offering tipping and dropping over time schemes that provide solutions to meet new M&A market trends. ROL in the US has remained higher, sometimes even double those observed in Europe and Australia. In addition, retention schemes tend to provide insurers with a great level of protection, often being set in the range of 2-4 percent of the enterprise value.

Cowhey: As a developing market, the transactional insurance product is dynamic, and pricing has evolved and become more competitive over time. Perhaps even more noteworthy, however, is the investment by some insurers in their development of an efficient and effectively staffed platform with a team of experienced professionals capable of dealing with complex and potentially multijurisdictional issues, all with the ability to keep up with the deal and offer a solution in 'deal-time'. Those insurers that have made such a commitment are now not only better able to provide timely response, but also have been able to streamline both the underwriting process as well as to consider provision of an underwriting solution for issues that

> **"As a developing market, the transactional insurance product is dynamic, and pricing has evolved and become more competitive over time."**
>
> *Jeffrey Cowhey, Ambridge Partners LLC*

may have once been the subject of an exclusion to the transactional insurance policy. In terms of geographic pricing, the transactional insurance market is becoming increasingly efficient, with markets contemplating the impact of local law, regulation and practice. As a result, the prospective user of R&W insurance for a typical North American transaction might expect to pay a bit more in premium than a user interested in securing W&I insurance for a European transaction.

Hendry: Underwriters consider many factors to determine pricing and coverage. These include governing law of the agreement, industry sector and geographic footprint of the target, quality of the deal advisers, past performance of the target, wider macroeconomic factors, proportion of the seller's 'skin in the game', plus numerous others. Ultimately, however, the transactional insurance market is exactly that, a market, and it will react to market forces, such as competition from other insurance providers, availability and access to capacity and the level of business in the market. As a consequence, pricing, policy retentions and coverage will fluctuate based on the nature of the underlying transaction and also competitive market pressure. There are distinct markets for transactional insurance around the globe, with material differences in coverage and pricing. While local legal, accounting and other M&A factors have an influence, the markets to a certain extent have developed independently of each other

based on the local market practice and attitudes of the practitioners.

DeLott: In recent years, the products generally have become less expensive and the terms more generous. I would expect that trend to continue as a number of new carriers have entered the market, bringing additional competition. And generally, the products are considerably less expensive in the UK, but the coverage is not nearly as broad.

RC: What impact has transactional insurance had on the due diligence process? With M&A projects being time-critical, to what extent does transactional insurance help free up deal teams to focus on headline issues?

Hendry: Transactional insurance is not intended to reduce or replace the processes that the parties would normally undertake and the expectation of the insurers is that disclosure and due diligence will be as robust as possible. One of the key advantages of W&I insurance is that both the seller and buyer can achieve comfort around the fact that the breach of warranty risk will be transferred to the insurer. Transactional insurance therefore can shorten the negotiation between both parties which can enable the legal, financial, tax and commercial teams to focus on the key issues.

DeLott: In my experience, the use of transactional insurance has not materially altered the due diligence process. Buyers want to know of any problems with the company they are buying, even when there will be transactional insurance. Note that the buyer will still have 'skin in the game' via retentions – or deductibles – and policy limits. Moreover, if the carrier is not convinced that adequate due diligence was performed, that is likely to negatively affect the terms of the insurance.

McBrearty: TRI is underwritten on the basis of having carried out a good and thorough due diligence and disclosure process. It is key to get the proper suite of due diligence reports in order to be able to underwrite TRI. When vendor due diligence is in place and insurers are granted access, the process is facilitated and accelerates. As such, for example, a significant part of the underwriting process can be carried out in advance of the buyer bidding at auction. We are not in a market where the due diligence exercise can be replaced by TRI. Having insurers in the loop certainly helps due diligence, however, as it allows another pair of eyes to look over the process and risk assessment. It is fair to say that, as insurers, we approach some issues from a different angle and as such, can bring a new approach or a solution to the negotiating table.

Cowhey: A frequent comment among those contemplating transactional insurance has been whether its use might lead to a reduction of buyer focus on completion of a robust due diligence undertaking. On the contrary, transactional insurance can provide an unintended benefit of enhancing the due diligence process as the underwriter's review of data room and diligence materials might serve as another set of eyes overseeing the transaction diligence process. The use of experienced transactional insurance underwriters will provide the parties with another seasoned team analysing both the process and conclusion of the diligence providers. By working with a familiar, experienced and dedicated underwriter, the buyer or seller should expect to find a professional looking to assist in the process of bringing the transaction to a timely close.

> **"It is key to get the proper suite of due diligence reports in order to be able to underwrite TRI."**
>
> *Deborah McBrearty, Tokio Marine HCC*

RC: Do you believe transactional insurance will become a mainstay in the arsenal of tools used by buyers and sellers to structure and close M&A transactions? What, in your opinion, gives transactional insurance the edge over traditional indemnities?

DeLott: In many cases, for commercial reasons, buyers will prefer to bring claims under transactional insurance policies rather than to litigate against sellers over breaches of reps and warranties. A good example would be where the management personnel responsible for the reps and warranties at issue have continued to run the acquired business and now work for the buyer. Or the buyer and seller may have other ongoing business relationships that could be adversely affected if the buyer were to pursue indemnity claims against the seller.

McBrearty: TRI is being taken up frequently and is considered, in many jurisdictions, an integral part of a clients' tool box. More parties are seeking quotes for insurance at the early stages of a deal process, which they then disclose in the data room. They then gauge bidders' interest with the two scenarios, with or without TRI. More often than not they gain more interest when including the TRI product. At the end of the day, the transfer of risk for a fixed priced and limitation of obligations from the seller's side are key, allowing a clean exit situation and differentiating TRI from other traditional collateral protections, such as escrow, that are tied up over time. In the past, dealmakers would talk about using W&I as a means of gaining a strategic advantage in a deal; nowadays, it can be argued that buyers will be at a strategic disadvantage if they do not consider using W&I insurance as part of a bid.

Cowhey: The use and acceptance of transactional insurance has grown exponentially over the past five years. In fact, it has become common for certain transactional professionals to be avid and repeat users of the product, as they seem to have embraced the ability to utilise insurer capacity to help facilitate a transaction. Given ascending rates of growth in both insured deals and a continuously growing list of transactional professionals that are users of the product, the continued growth of transactional insurance appears likely. This growth in repeat use appears to indicate a perceived advantage in the use of transactional insurance which may derive from the user's belief in the ability to enhance the terms of a transaction by providing greater certainty and potentially less indemnification obligation for the seller, while maintaining a sound tool for buyer recovery in the event of a breached warranty or representation.

Hendry: In the last seven or eight years, transactional insurance has grown at a rate of

over 20 percent year on year. It has proven to be increasingly popular among both buyers and sellers when structuring transactions, as it enables the free flow of consideration and offers a mechanism for getting deals across the line. In a survey we conducted in 2015, almost one in 10 private M&A transactions in the US and the UK used some form of transactional insurance. While there are plenty of buy-side motivations, it is as important for the sellers to have a good understanding of the solution to ensure that they achieve a 'clean exit'. Given this, and given its growth in recent years, it is our opinion that for the right deal it makes good economic sense to use transactional insurance rather than traditional indemnities, escrows or guarantees. Furthermore, the increased familiarity with transactional insurance among M&A practitioners, together with fulsome coverage and improved pricing, continues to drive its use.

RC: How do you expect the transactional insurance market to develop over the years ahead, in terms of take up, product development and other innovations that will benefit dealmakers?

McBrearty: Price, flexibility in the scope of cover, and the responsiveness and professionalism of insurers are factors that have already evolved and improved over recent years. They will continue to do so as competition swells. New areas of cover are emerging too. Areas which were traditionally excluded by insurers, notably in the tax sphere, such as transfer pricing in some jurisdictions, are now up for discussion. Environmental identified issues, such as pollution, is also an area where developments can be anticipated and new territories are already being explored. Different sectors of the M&A market are also ripe for development; just as we have seen an explosion of the use of W&I policies on real estate transactions, we could also see a similar increase in use in the distressed business, restructuring and turnaround market.

Hendry: There is still plenty of scope for the current products to grow. Not only do they provide sellers and buyers with an efficient and economic means of transferring deal risk, but it has been demonstrated on numerous occasions that insurers react positively to claims and have regularly settled valid loss. We see the scope for specialisation continuing to grow. There are certain underwriters that differentiate their product offering in the real estate and renewables sectors, through their sector knowledge and analysis. The healthcare sector is a good example of how the market is developing expertise and processes to understand the risks and provide effective cover. Additionally, we deal with insurers that focus their underwriting appetite at different deals levels, some preferring transactions where they can deploy a minimum of $40m of policy limit, whereas others concentrate on smaller

transaction values. It is going to be interesting to see how the claims history develops and also what impact the increasing prevalence of insurance will have on the underlying transaction process and behaviours.

DeLott: I believe the market for transactional insurance will continue to grow as more buyers and sellers have favourable experience with the product. And as more insurance carriers continue to enter this business, there are likely to be new products as carriers attempt to differentiate themselves.

Cowhey: Based on the sustained level of increased uptake of transactional insurance, as well as the continued growth of investment by select members of the transactional insurance marketplace, I would anticipate continued growth in the use of this insurance product. This growth will also be fuelled by continued development of enhancements in coverage and innovation, such as in areas pertaining to intellectual property, healthcare and other fields. Changes in the transactional insurance market will continue to streamline the process and to enable more efficient completion of business transactions.

RC: What final advice can you offer to parties involved in an M&A transaction, who are considering transactional insurance?

Cowhey: I would encourage the prospective user of transactional insurance to develop an ongoing trading relationship with one or more insurance professionals, both broker and underwriter, in order to build a familiarity with that prospective insured's due diligence process, its procedures, and its internal and external capabilities. This familiarity can breed efficiency if the underwriter can see a common trend of a procedure-driven and robust diligence process and could help to further streamline and economise the insurance procurement process.

> **"In the last seven or eight years, transactional insurance has grown at a rate of over 20 percent year on year."**
>
> *Brian Hendry,*
> *Paragon International Insurance Brokers Ltd*

Hendry: Parties should factor transactional insurance into the deal at an early stage. While markets have evolved to react at speed, there are many benefits to affording the insurance process more time. This way the parties can gain a broad understanding of the risks the insurance products can deal with, but as importantly, what risk may fall outside the scope of the policy – with the benefit that there is no commitment to buy insurance at an early stage of the process. If there are issues that could potential disrupt the deal, there will be time to investigate if there is an insurance solution to overcome the hurdle and consider the options that are available in the market. Positioning yourself early allows for the underwriting process to be streamlined to be run in parallel with the transaction timetable and ensures that the parties are safe in the knowledge that the insurance will commence as soon as the deal completes.

DeLott: A final word of advice would be to engage with a broker and a legal adviser with significant experience in negotiating these products. By now, the major insurance brokers and the leading law firms all have personnel with significant experience in negotiating transactional insurance policies.

McBrearty: In order to benefit fully from TRI, we recommend considering this insurance early on. Anticipation is key. When insurers are brought in earlier enough they can work alongside the client, offering back-to-back cover to the fullest extent possible before the sale & purchase agreement is finalised. By assessing the risks from their perspective, insurers also shed light on negotiations, helping to bridge the gap sooner and facilitating the deal process. R&C

PERSPECTIVES

STEMMING THE TIDE: DELAWARE'S COURTS AND LEGISLATURE TAKE AIM AT DEAL LITIGATION

BY **BRIAN HOFFMANN AND SCOTT REGAN**
> MCDERMOTT WILL & EMERY LLP

For the better part of a decade, mergers and acquisitions (M&A) involving publicly-traded Delaware entities have been plagued by over-exuberant litigators exploiting well-meaning law. Shareholder suits hit their peak in recent years, with shareholders challenging more than 93 percent of deals valued at over $100m during each of the years 2011 through 2014.

Through the first half of 2016, however, in the wake of shifts in several areas of Delaware law, Delaware entities have been the beneficiaries of a precipitous drop in shareholder challenges. Thus far, the total number of deals subject to shareholder litigation has fallen by more than 57 percent from the first half of 2015, and even deals valued at over $100m have enjoyed a nearly 25 percent reduction.

This follows a more modest decline in 2015, which was the first year since 2009 that saw fewer than 90 percent of M&A deals valued over $100m challenged by shareholders. Mercifully, the most recent decisions of the Delaware courts and actions by the Delaware legislature seem to show a recognition that the previous mechanics were too susceptible to perverse profiteering, and may indicate a willingness to pave the way for deals down the road.

Spurred by several questionable incentives – including attorneys' fees in cases seeking mere supplemental disclosures and statutory interest in

appraisal arbitrage trials – activist shareholders and the plaintiffs' bar have run rampant against robust post-Great Recession M&A. With the costs of litigation so low and the returns almost guaranteed, Delaware entities have taken it as a given that any M&A deal they may consummate will be affected by litigation. Indeed, such challenges have become so commonplace that the expected cost of a lawsuit is often included in the deal price, with both sides acknowledging that the lure of litigation is simply too great. For many years the Delaware courts and legislature had stood their ground, reluctant to disrupt the status quo. Recently, though, both have responded.

The most devastating blow to the status quo was delivered by the Delaware Supreme Court in *In re Trulia, Inc. Stockholder Litigation*. *Trulia* capped off a string of cases first questioning and then outright denouncing 'disclosure-only' settlements that had been clogging the Delaware courts. In these cases, suit is brought, usually targeting the largest transactions at the early stages of a deal, with the ultimate aim of attorneys' fees and a mere non-monetary settlement.

In exchange for fees and disclosures, the defendant corporations typically receive a global release of claims relating to the underlying transaction. Functionally, this outcome offers almost no discernible benefit to the shareholders on whose behalf the suit was instituted, although defendant corporations enjoy the ancillary advantage of precluding more damaging suits later on. Still, the process has been nettlesome for defendant corporations and even more bothersome for courts tasked with assessing and approving these settlements.

After the earlier *In re Aruba Networks, Inc.* and *Acevedo v. Aeroflex Holding Corp*. decisions, in which the Court of Chancery analysed the perverse symbiosis of plaintiffs' lawyers getting their fees, defendant corporations getting broad releases, and shareholders getting no discernible benefit and found the proposed settlements inadequate and the underlying cases to lack merit, the door was open for the court to quash these questionable suits in *Trulia*. The court did not disappoint. In *Trulia* the court rejected the proposed settlement to the merger challenge and excoriated the plaintiffs, who it reasoned were motivated only by fee-grabbing and not by any concerns for the shareholders at large.

Indeed, building on the decision *In re Riverbed Technology, Inc. Stockholders Litigation* where Vice Chancellor Glasscock expressed barbed scepticism of shareholder value from disclosure-only settlements and questioned the court's "formerly settled practice" of approving them, the court went so far as to state that these cases often serve "no

useful purpose" and may subvert the adversarial process itself. This strong language has been echoed in cases in other courts since, including the 7th Circuit, which, in its recent decision in *In re Walgreen Co. Stockholder Litigation*, forcefully concluded that this "type of class action... is no better than a racket. It must end."

The effects in Delaware have been immediate, as these suits have become far less prevalent, even as other state courts that have yet to adopt *Trulia* have endured an uptick. Moreover, the Chancery Court has already relied on *Trulia* – and the notion that, where the sales process was sound, claims are mooted once the defendant corporation makes the disclosures demanded by the stockholders – to reduce one fee award from $275,000 to $50,000; sending a strong message to plaintiffs' attorneys to make sure they have a "good bull", in Vice Chancellor Glasscock's words, before proceeding with suit.

Only a few months after the *Trulia* decision, in *In re EZCORP Inc. Consulting Agreement Derivative Litigation*, the Delaware Chancery Court added uncertainty to the viability of certain shareholder suits. Before EZCORP, several Delaware decisions, including *Rabkin v. Olin Corp., In re Wheelabrator Techs., Inc. S'holders Litig.,* and *Kahn v. Lynch Communication Systems, Inc.*, had held that the onerous "entire fairness" test applied to transactions involving a controlling shareholder.

However, Delaware case law also provided an exception in change-of-control transactions involving a controlling shareholder whereby the deferential business judgment rule could supplant entire fairness if the corporation relied on both a truly independent committee and a majority-of-the-minority vote. With *EZCORP,* the Court of Chancery transformed this exception into the rule.

"Activist shareholders and the plaintiffs' bar have run rampant against robust post-Great Recession M&A."

Although *EZCORP* did not involve an M&A deal, the roadmap laid out by the court applies to any transaction involving a controlling shareholder. While the court indicated that entire fairness will apply in many cases, it also sanctioned the previous exception's procedure for replacing this standard with the board-friendly business judgment rule. Thus, if, from the outset, the transaction was subject to approval by a fully authorised and

effectively functioning committee of independent and disinterested directors and by an unwaivable majority of the minority shareholders in a fully informed vote, then the business judgment rule should apply, regardless of the transaction at issue.

While the availability of entire fairness review has made shareholder suits in these contexts particularly attractive because of the high burden imposed on defendant corporations to prove both a fair price and process, by muddying the waters and outlining a process for earning court deference, the court has potentially discouraged some suits that are worthwhile only if the odds are stacked in the shareholders' favour.

Outside of the courtroom, the Delaware legislature has also been active in combating the perverse incentives it helped create. Just this summer, effective 1 August, the legislature amended the Delaware General Corporation Law (DGCL) to restrict and disincentivise shareholder appraisal suits. In effect, the amendments: (i) limit appraisal rights to shareholders who have, at a minimum, a $1m stake in the company or own at least 1 percent of the company's shares; and (ii) permit companies subject to appraisal actions to prepay any desired amount on the merger consideration (which would be credited toward any final judgment of the court and would not be subject to the prejudgment interest rate which has attracted suits in recent years).

With hedge funds dominating appraisal suits and interest accounting for about 60 percent of the return in appraisal trials between 2000 and 2014, these amendments are targeted directly at the appraisal arbitrage strategy of holding a small number of shares to reap the reward of high interest rates. Analysis conducted by Wie Jiang of Columbia Business School et al. preceding the passage of the amendments predicted that the 'de minimis' amendment would precipitate a 23 percent drop in appraisal filings, and, if the legislature's theory holds, the interest rate amendment could compound the impact.

While it is far too soon to know the true effect of these amendments, corporations and their counsel have welcomed the legislature's willingness to push back against shareholder suits. Especially after a 2015 amendment to Sections 102 and 109 of the DGCL prohibited fee-shifting provisions in bylaws and certificates of incorporation – one of most effective instruments corporations had devised for thwarting illegitimate litigation – 2016's amendments demonstrate a newfound awareness of plaintiffs' incentives and the questionable usefulness of many shareholder suits. Together with corporations' ability, under the recently amended Section 115 of the DGCL, to make Delaware the exclusive jurisdiction for all internal corporate claims, these latest amendments may pack a punch.

Together, the latest legislative actions and the Delaware courts' long-awaited willingness to deter the tidal wave of shareholder strike suits may be an effective antidote to the litigation excesses of

the past 10 years. Still, although we have observed a sharp decline in shareholder litigation since the end of 2014 and current developments indicate a desire to make litigation less attractive to would-be antagonists, it is likely too early to predict an enduring ebbing of strike suits against M&A deals. Considering M&A's continuing centrality to economic growth when organic growth is difficult, however, for the time being the curtailment of these lawsuits should be a welcomed reversal across all industries. R&C

Brian Hoffmann
Partner
McDermott Will & Emery LLP
T: +1 (212) 547 5402
E: bhoffmann@mwe.com

Scott Regan
Associate
McDermott Will & Emery LLP
T: +1 (212) 547 5703
E: sregan@mwe.com

PERSPECTIVES

DEVICES AND DATA: THE ENTERPRISE FRONTIER

BY **NIC SCOTT**
> CODE42

In the enterprise space, bring your own device (BYOD) is not a new concept. With technical strides forward in mobility and internet access virtually everywhere, employees are now accessing corporate information on numerous devices across a variety of locations. Combined with the 'always-on' mindset of 21st century business, employees have the scope to get tasks done more quickly than before. However, with increased connectedness comes increased security concern.

The days of sensitive corporate information being safely tucked away in the data centre are long gone. Essentially, every mobile device, every laptop and every desktop used by employees to store business information could be a potential entry point for a hacker or piece of malware.

So how much corporate data is actually stored at the endpoint, and is it really worth the investment to keep it safe? According to UK-based CIOs and CISOs surveyed in our recent Datastrophe Study, up to 47 percent of corporate information is stored at the endpoint today. Needless to say, the downtime or potential fallout for that much company data falling into the wrong hands or being corrupted could destroy a business, so adequate security is a must.

Many companies today know this, and as a result they have set up a clearly defined BYOD policy. In fact, 65 percent of IT decision makers (ITDMs) have one in place and communicate it effectively to the

rest of their organisation. Or do they? Interestingly, knowledge workers take a slightly different view, with 67 percent disagreeing with ITDMs, suggesting their organisation does not have clear rules about devices in place.

This disparity between what IT and knowledge workers believe is the problem facing the enterprise today. Neither party can effectively safeguard company information without a clear view of what is and is not acceptable when it comes to handling corporate data. As technological advancement continues apace, it is important for ITDMs to create forward-looking BYOD strategies, and then ensure that every single person within their organisation knows it back to front.

Step 1: Ownership, classification and communication

When employees are using their own tablet, mobile or laptop for work, they are of course likely to have a greater feeling of ownership compared to a work device. For this reason, it is understandable that they should want to keep these devices safe, and thus may be more risk averse as a consequence. ITDMs can take advantage of this mindset by devising a BYOD policy that clearly outlines some of the potential dangers when it comes to where and how data is stored. Of course, in order to do this successfully, it is important to establish the risk level of each type of data – as obviously not every kilobyte will be integral to the business.

Valuable data that is considered vital to the organisation should be classified as 'mission critical' and held on the premises for maximum security, while information that is considered less high-risk could be authorised for storage on a public cloud service. This is referred to as a 'hybrid' cloud service and can give organisations the best of both worlds in regard to storing information. Categorising data via importance allows for particularly sensitive data to be kept on-premise and away from the endpoint – where it would traditionally be more at risk.

After data categorisation, the next stage is implementing user-friendly storage and modern endpoint backup technology. Appropriate ring-fences for specific data types should be set-up. Then, ITDMs must successfully communicate where and how knowledge workers should be storing their information without violating company regulations. If the organisation chooses the right technology from the start, then it will be far easier for employees to buy-in to the data security policies implemented, thus taking it all the more seriously.

> **"Sometimes the insider threat goes beyond the removal of company data and IP and takes the form of complete removal or destruction."**

Step 2: Keeping an eye on the blind spot

Even when knowledge workers are using their own devices responsibly and adhering to BYOD policy, the security threat does not go away. There will always be bad apples in large organisations, as well as unwitting actors, both of whom will put

corporate information at risk by ignoring the rules and practising 'Shadow IT'.

The key to managing the 'insider threat' presented by knowledge workers using their own devices and unapproved third-party solutions is to have security tools in place that allow ITDMs to spot abnormal data activity at the endpoint. The right solution should defend against both internal and external types of breaches, such as when malware has infected a machine and is harvesting data, or when credentials have been literally handed to a hacker, either intentionally or unwittingly. Regardless of how it happened, if there is a situation where something looks suspect at the endpoint, it is important to detect and respond accordingly.

The big challenge here is how to detect the abnormal activity. To start with, ITDMs need to understand what the normal state looks like. This is done via advanced analytics and other technologies that look at things such as when an employee regularly logs in and out during work hours, transference of files into approved third-party solutions, or sending a certain amount of emails per day. Then, should this behaviour suddenly change dramatically (for example logging in at 3:00am and firing off a large amount of data to an unknown IP address), then it will raise a red flag.

Identifying this behaviour is only half of the battle. It is also important to see exactly what has been sent, its current state, specific version history, and so on, so the right information can be given to stakeholders or authorities in the event of a breach. Fortunately, this can be achieved by the more advanced endpoint monitoring tools on the market.

Of course, sometimes the insider threat goes beyond the removal of company data and IP and takes the form of complete removal or destruction. In these cases the detection of this activity is the first step, with the second being the ability to quickly and easily restore the lost information via modern endpoint backup.

In order for ITDMs to gain support for internal profiling of either personal or work devices it is important to shift the focus away from distrust and 'keeping an eye on people'. Instead, it should highlight the need to find the anomalies that contribute and lead to internal data breaches. If this is communicated well, it will not be seen as a 'big brother' approach, but rather keeping employee devices safe through active safeguards.

Step 3: Covering all bases

Brexit has created a volatile environment in the UK both technologically and politically. There are many unknowns in regard to upcoming legislation such as the Investigatory Powers Bill, General Data Protection Regulation (GDPR), and the recently implemented Privacy Shield.

In times of uncertainty such as these, it would be foolhardy for ITDMs, and indeed CSOs and CISOs, to rest on their laurels and wait and see what happens prior to implementing appropriate tools and data

policy, BYOD rules included. The threat of factors such as shadow IT and external hackers certainly will not wait, and neither should organisations.

Unfortunately, no company is 100 percent bulletproof when it comes to safeguarding against data loss. However, with the right security tools, training and policy in place, the risk can be dramatically lowered. ITDMs should implement a full stack of security solutions, from breach detection, antivirus and endpoint monitoring as first-line defence, and modern endpoint backup as last-line remediation.

A company's most important assets are its data and its people, with the two more intertwined than ever before. In 2016, organisations need to dedicate as much time as possible to keep both safe, and the latter updated and informed. Do this, and regardless of what happens in the world outside, at least you will have your internal bases covered. R&C

Nic Scott
Managing Director UK & Ireland
Code42

PERSPECTIVES

WHEN IT COMES TO HUMAN CAPITAL REPORTING, MUM'S STILL THE WORD

BY **HAIG R. NALBANTIAN**
> MERCER WORKFORCE SCIENCES INSTITUTE

The idea that an organisation's workforce is an 'asset' rather than simply a business cost is now broadly embraced by corporate leaders everywhere. Quite a few of them even declare, in their annual reports, that it is their organisation's 'greatest asset'. How remarkable then, that in those very same annual reports a proper accounting of the size, composition and management of the greatest asset is nowhere to be found.

This omission should be of concern to the investment community and those charged with regulating capital markets, because the evidence is mounting that substantial value is at stake in getting human capital management right. For example, a study of the US manufacturing sector found strong, positive relationships between sustained advantages in workforce productivity and the market value of companies, as measured by Tobin's Q, the ratio of the firm's market value to the replacement value of its capital assets. In effect, a consistent advantage in workforce productivity was found to function as an intangible asset for companies. But what explains differences in workforce productivity?

In our experience, human capital management is a significant, measureable driver of variations in workforce productivity in organisations, and often the most important avenue to sustained productivity advantages.

For example, in a large hospital system, statistical analysis showed that about 63 percent of the

variation in relative workforce productivity across hospitals within the system and over time was attributable to human capital management, and not to differences in financial capital, technology or the vintage of equipment.

What really mattered were factors relating to the composition and management of the workforces in these facilities – factors such as the quality of staff, part-time/full time ratios, management ratios, supervisory spans of control, overtime utilisation and turnover. Simply optimising part-time utilisation across the system was estimated to be worth 3 percent of revenues annually, a large amount for a healthcare organisation straining under reduced reimbursements. Optimising across all key management levers would net much more.

Other examples tell a similar story. In a large national retail chain, human capital factors accounted for nearly 40 percent of the variation in store profitability. In a US regional bank, the impact of human capital varied from a low of 10 percent to a high of over 40 percent depending on the performance measure analysed. The message is clear: while its relative contribution varies across industries and even across companies within industries, human capital management matters – often a great deal.

The absence of meaningful reporting on human capital management has not gone unnoticed. Over the past two decades there have been serious efforts in various jurisdictions to get human capital out of the shadows. Some have emanated from the financial accounting world, some from the 'sustainability' or the Environmental, Social, and Corporate Governance (ESG) world. And various investor groups, whether they be government or private pension funds, shareholder activists or responsible investment (RI) organisations, have been pressing hard to get meaningful human capital reporting standards put in place.

Thus far, these efforts have come

up short. All too often, the annual reports of publicly traded corporations still resort to boilerplate commentary about their organisation's human capital. Almost nowhere does the information provided about the company's workforce and the way it is managed bear any resemblance to what is reported on physical, financial and 'relational' assets (e.g., 'goodwill'). To date, there is still no commonly accepted standard on what organisations should report about their workforces.

Achieving consensus on a set of standardised measures of human capital management to be publicly reported has proven elusive, for good reason: determining the right measures to report to shareholders is a challenging task. The problem lies in the highly contextual nature of human capital management. Indeed, effective human capital management is far less about 'best practice' or adherence to some external benchmarks than it is about 'best fit'.

Practices that work well in one environment may fail miserably in another. For instance, 'pay for performance' or variable pay is commonly regarded as an important instrument for enhancing employee motivation. Countless executives proudly proclaim that their organisation's reward systems are 'results oriented', yet there is substantial evidence that the impact of variable pay schemes is highly dependent on a variety of contextual factors, such as the volatility of the performance measures to which payoffs are tied, the way work is organised and the structure and intensity of supervision, among other things.

This helps explain why variable pay programmes have very high variance in their effectiveness. Sometimes they contribute enormously to higher performance. Sometimes they actually diminish performance. This variance is due fundamentally to problems of systems 'fit', not plan design. All too often, variable pay plans are put in place in an environment

where they cannot possibly succeed because other management practices or contextual factors are arrayed against them. Simply knowing the incidence and extent of pay for performance in a firm says little about the efficacy of rewards, let alone human capital management, in organisations.

Even the most basic measures of human capital management can be highly misleading if not assessed in context. For example, employee turnover is often looked at as an important measure of how well an organisation is managing its workforce. If employees are leaving at relatively high rates, something in the employment proposition must not be working. Moreover, turnover imposes costs on organisations.

Common bottoms-up approaches to estimating the cost of turnover, taking into account the resources expended on recruitment, selection, hiring, on-boarding, training, as well as the ramp-up time for employees to reach reasonable levels of productivity and the resulting disruptions to work and teams, suggest turnover is very costly – with estimates varying from 50 percent of pay for non-exempt hourly employees to 150 percent or more for salaried staff. By these calculations, how could one not conclude that lower turnover is 'better' than higher turnover and that management teams that maintain low turnover are holding labour costs down and securing gains for shareholders?

But conclusions based on such bottom-up calculations may be misleading. Employee turnover can have important positive effects as well: it can help weed out poor performers and open up positions for up-and-coming talent. Most importantly, turnover may be a vital instrument to speed adaptation of organisations to changing business needs. In today's economy, business strategies and conditions are constantly changing, due to competitive forces, advances and shifts in technologies, customer needs and values. Inevitably, these require changes in an organisation's workforce as well.

> **"Even the most basic measures of human capital management can be highly misleading if not assessed in context."**

In periods of transition, higher turnover may be necessary to enable the kind of workforce transformation required to drive business success. Those organisations that make the required shifts more fully and quickly will outperform those that lag. As such, higher turnover may be a better predictor of

business success than lower turnover. It is surprising how often the problem in organisations is too little turnover, not too much. Simply reporting out turnover rates without providing information on the contextual factors that permit intelligent interpretation of this measure can be seriously misleading.

As these examples demonstrate, when it comes to human capital management, what matters most is how well-aligned workforce practices are with each other and with the strategic goals of the organisation. Unfortunately, measuring 'best fit' is a far more complex endeavour than measuring alignment with so-called 'best practice'. Given the challenges of creating 'best fit' measures, is the effort to create universal standards for human capital reporting a lost cause? We think not.

The goal of human capital reporting should be to provide information by which investors can gauge whether the organisation is securing the right workforce – the right mix of skills, capabilities, and experience – and whether it is managing that workforce in a way that drives productivity. To make this determination, investors need to have some knowledge about the methods and processes used by company management to ensure human capital is, in fact, being managed as an asset and managed effectively.

Key questions include: (i) does the organisation have in place an explicit workforce strategy that defines the set of workforce 'assets' required to achieve business goals, and a set of consistent, mutually-reinforcing management practices designed to ensure these assets are secured and productively managed?; (ii) what are the core elements of this workforce strategy?; (iii) on what is this workforce strategy based? Specifically, what kind of quantitative and qualitative information is management relying on to inform its workforce decisions?; (iv) what measures are in place to track whether the strategy is being executed effectively?; (v) are these measures being used to hold executives and line leaders accountable for results?; and (vi) what processes and measures are in place to identify potential or looming risks to the organisation's human capital and what institutional structures or practices can be called on to mitigate any risks identified?

Rather than mandate a specific set of metrics to be reported by all, it may be preferable to oblige management to provide responses to process questions such as these, backed by hard data to substantiate their answers. This would represent a huge improvement over the status quo. It would enable investors to distinguish companies that pursue a disciplined asset management approach to human capital from those who do not.

Competitive pressures to convince investors of the efficacy of their human capital management would spur management teams to make their reporting on human capital meaningful and compelling. And yes, the delineation of process envisioned here could be complemented by reporting on some basic measures of human capital management that have

universal value and social significance – for example, measures relating to workforce demographics, pay equity, employee engagement, workforce productivity and innovation.

But these metrics would not be rendered in a vacuum. They would be but a part of a larger narrative designed to help investors understand the logic of the company's approach to human capital and, in the process, to make management teams themselves focus on the right questions and pursue their answers in the right way.

For many organisations, human capital is the largest single investment they make and the one they know least about. Fortunately, pressures are mounting for this to change. Advances in workforce sciences, the proliferation of workforce data easily accessed from Human Resources Information Systems (HRIS), and the rapid strengthening of workforce analytics capabilities make it possible, finally, for organisations to apply an asset management discipline to their human capital. Many companies have started to pursue this journey. In fact, many larger organisations are now creating in-house analytics functions to help guide management decisions about their human capital.

We are living in the age of human capital, where an organisation's workforce – both who it is and how effectively it performs –- is often the principal and only enduring source of competitive advantage. In the face of this reality, it is imperative that organisations provide capital markets meaningful information about their human capital. Investors cannot possibly make informed decisions if they are in the dark about companies' management of their human capital assets. Greater transparency about human capital management is in the interest of workers too. Formally elevating labour to an 'investment' category recognises its importance to creating value and helps overcome the outmoded positioning of labour as the 'variable' cost of production.

Developing effective standards for human capital reporting is both the next frontier in the management of human capital as a discipline and the logical consequence of the changing nature of labour's contribution to the creation of economic value. Investors should be encouraging this development and leading the charge to have publicly-traded companies provide the information they need to make wise investment decisions. R&C

Haig R. Nalbantian
Senior Partner
Mercer Workforce Sciences Institute
T: +1 (212) 345 5317
E: haig.nalbantian@mercer.com

PERSPECTIVES

STUDY IN CONTRASTS: DEMOCRATS AND REPUBLICANS ON HR POLICY

BY **JIM O'CONNELL**
> CERIDIAN

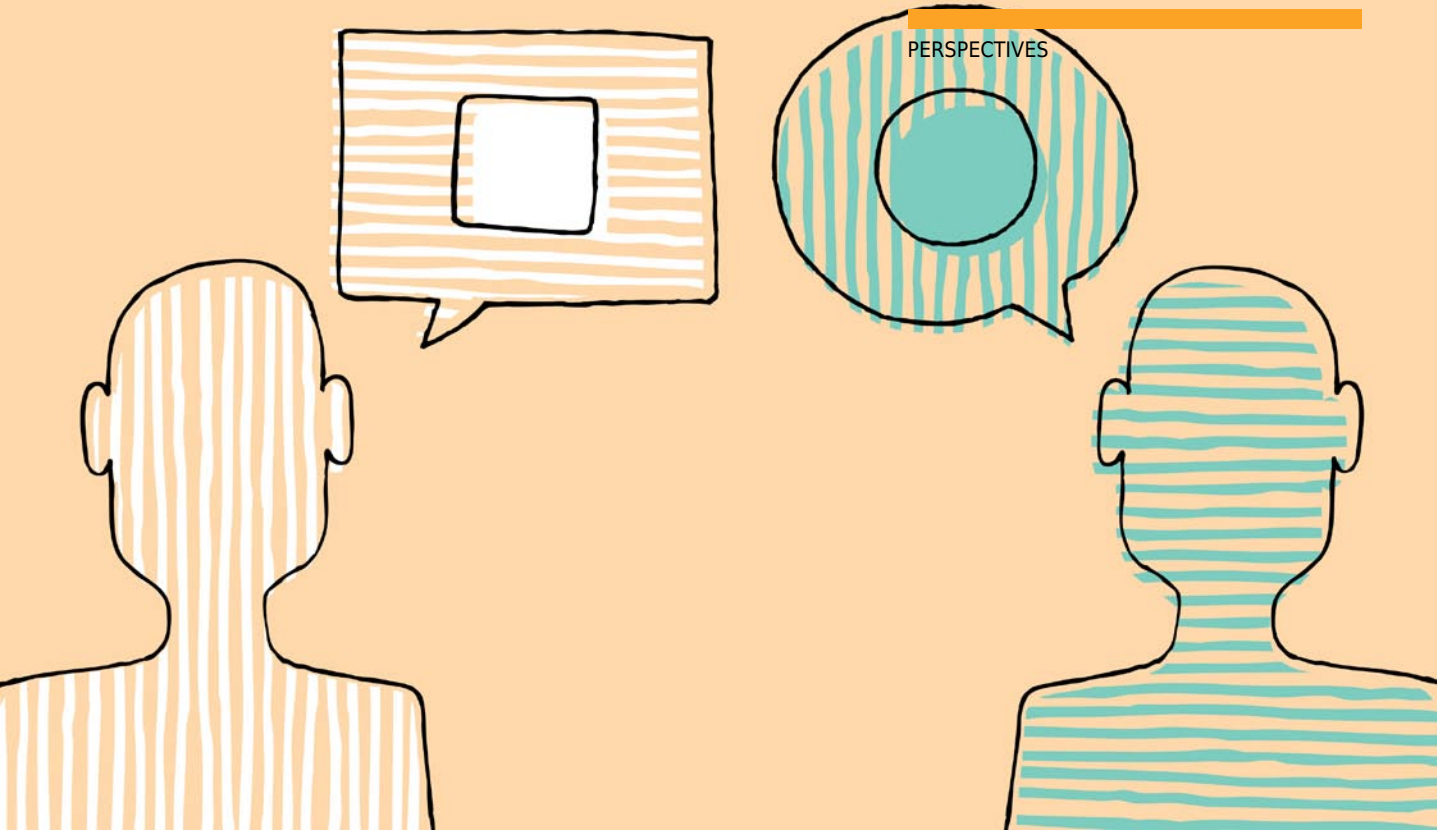
On 8 November 2016, Americans will go to the polls to elect Democrat Hillary Clinton or Republican Donald Trump the next president of the United States. In the key area of human resources policy, the views of Democrats and Republicans are a striking study in contrasts.

Affordable Care Act

Six years after enactment the public remains divided on the ACA, with about half of those surveyed having an unfavourable view of the law. In their competing plans Democrats and Republicans reflect that divide.

Democrats. The Democratic platform embraces the ACA, calling it "a critically important step toward the goal of universal health care", and are "proud to be the party that passed the Affordable Care Act". The party would double-down on the law or, as Mrs Clinton puts it, "build on the ACA".

Specifically, the platform calls for three big changes. First, adding a 'Public Option' to the federal and state health insurance exchanges, i.e., giving the 10 million or so enrollees the option of selecting a Medicare or Medicaid-like health plan instead of a private insurance plan. Second, "keeping costs down by making premiums more affordable, reducing out-of-pocket expenses and capping prescription



drug costs", presumably by expanding the present government-financed premium tax credits or cost-sharing reduction subsidies. Finally, repealing the ACA's 40 percent excise tax on high-cost health insurance, known as the 'Cadillac Tax', slated to go into effect in 2020. The platform is silent on what might replace this $90bn, 10-year funding source for premium and cost-sharing subsidies.

Republicans. While 'repeal' is the GOP's bumper-sticker position on the ACA, it is more accurately described as 'The 4 Rs': Retain, Remove, Replace, Reduce. Republicans would retain some provisions; remove others completely; replace certain sections with competing ideas; and reduce, or scale back, other provisions. A few examples: ACA's ban on pre-existing condition exclusions would be retained; the Cadillac Tax no doubt would be removed; replaced would be the requirement that all exchange health plans offer a defined, 10-category 'essential health benefits' package; and likely reduced, or scaled back, would be the law's individual and employer mandates.

Isn't legislation needed?

The difficulty in the contrasting positions, of course, is that the proposed changes require Congressional approval, i.e., amendments passed by the House and Senate. To change the ACA, therefore, the new president will need to propose amendments, followed by negotiations between Capitol Hill Republicans and Democrats and ultimately a compromise package signed into law.

What will it mean for employers?

From an employer perspective, all the proposed ACA changes translate into ongoing compliance uncertainty. Will the Cadillac Tax be replaced by a new cap on the present law tax exclusion for employer-provided coverage? Would a public option in the exchanges be an attractive alternative? How would a President Trump scale back the employer 'play or pay' mandate? Would a President Clinton accept changes to the employer mandate to win support of other changes?

New ideas to further 'reform' the 2010 healthcare reform law guarantee that employers will face growing compliance complexity, consternation and risk – even as employers are expected to continue sponsoring comprehensive health benefit plans for employees and their dependents.

Mandatory paid leave

The Family & Medical Leave Act (FMLA), which recently marked its 23rd anniversary, entitles eligible employees to up to 12 weeks of job-protected unpaid leave for their own or a close relative's serious health condition. FMLA was one of the first pieces of legislation President Bill Clinton signed into law.

Almost since its enactment, however, Congress has been urged to reopen the law to require paid sick and family leave.

Democrats. The Democratic platform and Mrs Clinton's campaign speeches on this issue are unambiguous: "Democrats will make sure the United States finally enacts national paid family and medical leave by passing a family and medical leave act that would provide all workers at least 12 weeks of paid leave to care for a new child or address a personal or family member's serious health issue."

Mrs Clinton has said that as president she would propose legislation giving workers 12 weeks of paid leave and a minimum two-thirds wage replacement rate. Mrs Clinton's paid leave mandate would be financed by raising taxes on wealthy Americans, not by higher employee payroll taxes.

Republicans. The party has not been enthusiastic about government mandates and by every indication is unenthusiastic about requiring paid leave. Legislation introduced in the Republican-controlled House and Senate in recent years to require seven days of paid sick leave, the Healthy Families Act, has gone nowhere. And shortly after being elected Speaker of the House, Rep. Paul Ryan (R-WI) said it "doesn't make any sense" for him to support paid leave legislation, observing that "I don't think people asked me to be speaker so I can take more money from hardworking taxpayers to create some new federal entitlement".

To be sure, Mr Trump does not always endorse Republican views and as president might support some form of paid leave legislation. And the official Republican platform does not address the issue.

Nevertheless, it is not likely that amending FMLA to mandate 12 weeks of paid sick or family leave would be a priority for a Republican Congress or White House.

Implications for employers

While the debate over paid leave percolates, some 30 states and municipalities have enacted variations on the theme of mandatory paid leave. This hodgepodge of often-conflicting employer mandates is a compliance headache for multi-jurisdiction employers.

Employers will be watching closely if the new president initiates paid leave legislation in 2017. Among other things employers will want to know whether the FMLA small business exemption remains, whether employees must work at least 1250 hours during the preceding 12-month period to be eligible and whether an employer's existing PTO policies comply. In any event, it seems inevitable that momentum will build for a national paid leave mandate.

Minimum wage increase

Amid growing concern about income inequality and wage stagnation, support has been growing for a substantial increase in the federal minimum wage, now $7.25 per hour or roughly $15,000 a year.

President Obama has proposed an increase to $10.10 an hour or slightly over $20,000 annually. Congressional Republicans, worried that a big boost in the minimum wage could increase unemployment, have scuttled the legislation.

> **"Employers small, medium and large have their seatbelts fastened for another polarising presidential election."**

Meanwhile, a 'Fight for $15' movement has gathered steam, as a number of state and local jurisdictions have raised minimum wages. California, for one, recently enacted a law to raise the state minimum wage to $15 (or $30,000 a year for full-time workers) by the year 2022. What are the positions of the presidential candidates on the issue?

Democrats. Increasing the minimum wage was one of the most hotly disputed issues in the Clinton-Sanders primary battle, with the Vermont senator advocating a $15 federal minimum and former Secretary of State Clinton, concerned about low-wage jobs, favouring something less. At the

Democratic National Convention in Philadelphia Mrs Clinton conceded the point to Senator Sanders. The first item on the Democratic Platform list of priorities, R*aising Workers' Wages*, states, "We should raise the federal minimum wage to $15 an hour over time..." With all the Democratic Party factions now coalesced around a $15 minimum wage, it would clearly be one of the first initiatives of a President Hillary Clinton in 2017.

Republicans. While the Republican platform calls for infrastructure modernisation, better job training, economic growth, lower taxes, cutting regulations, a 'Twenty-First Century Workforce' and a focus on human capital in 'getting the American people back to work', no mention is made of increasing the federal minimum wage. Mr Trump's position differs from the GOP's. The Republican presidential candidate recently stated that he would "like to raise [the minimum wage] to at least $10". With Democrats calling for a $15 federal minimum "over time" and Mr Trump suggesting he's open to "at least $10", compromise would seem possible. The minimum wage will ratchet up – the only question is when.

What employers should expect

For employers, of course, political uncertainty about the federal minimum wage, jobs and the escalator effect on other wages echoes uncertainty about the future of the Affordable Care Act and a federal paid leave mandate. A $15 minimum seems likely, with the debate mainly about a phase-in period and possibly flexibility for the president to delay effective dates depending on the state of the economy.

Conclusion

Employers understand that issues like health insurance, paid leave, minimum wage and the new overtime rules are parts of the same tapestry: human resources as a public policy priority. As employers evaluate the candidates' positions on these issues, they see the chasm that separates Democrats and Republicans on HR policies that affect so many Americans. Political consensus seems elusive, with compliance complexity, cost and risk an unfortunate consequence.

Employers small, medium and large have their seatbelts fastened for another polarising presidential election. They can only hope that post-Election Day Democrats and Republicans will rediscover a spirit of compromise – especially on the issues that affect America's most important resource: its people. R&C

Jim O'Connell
Compliance Analyst
Ceridian

PERSPECTIVES

COMMUNICATION IS MUCH MORE THAN TALKING AND WAITING TO TALK

BY **TONY BELAK**
> INTERNATIONAL CENTER FOR COMPASSIONATE ORGANIZATIONS (ICCO)

One of the most powerful aspects of being human is the yearning to be understood, and when we think someone listens, or we are taken seriously, and our ideas and feelings are recognised, and we have something of value to share, we can claim happiness.

Communication entails the ability to listen beyond the physiologic traits of hearing. Since listening is a learned skill, it can be retrained. Hearing is the autonomic or involuntary reaction of the nervous system and senses. Listening is a voluntary act that requires concentration and willingness. The listener's empathy, which is an understanding of what is being said and showing it, builds bonds and improves relationships, and the power of deep listening should not be underestimated.

Listening not only strengthens relationships by cementing connections with another, it also fortifies one's sense of self. As such, by giving an account of our experiences to someone who listens well, we can hear ourselves, identify our needs, and better see solutions or remedies. Listening is so basic it is often taken for granted. It is especially painful not to be listened to in those relationships we count on for understanding. We define and sustain ourselves through conversations with others, and the response is what makes our feelings, actions and intentions meaningful. Only a small proportion of the message is conveyed through words alone, while the tone

in our voice and gestures and other body language signals convey most of the message.

We can say something and send a very different message through non-verbal communication. This is why electronic messages read from a screen are often misinterpreted, so emoticons, emoji and other symbols are used to express an emotional content or soften what may be perceived as harsh words. Misunderstandings can be painful, and that hurt can trigger relationship toxification. Effective communication depends on clarity, speech pattern and the intonation conveyed by the sender of the message, as well as the ability of the listener to attend to the message. Effective listening is much more than just hearing; listening is the ability to receive and interpret verbal messages and cues, such as body language, in order to respond appropriately to the purpose and needs of the sender.

Training managers and supervisors to use productive communication styles, effective feedback and clarification, paraphrasing and listening for

feeling should be a priority, because a supportive climate occurs when both the speaker and listener feel their communication is characterised by open, non-judgmental, spontaneous and respectful behaviour. To this end, an effective listener may comment on the feeling behind the speaker's words or the feelings expressed through body language to show that the listener is supportive of the speaker's need to be understood.

It is enough to identify or affirm the appropriate emotion being displayed without need to explore the underlying cause of that emotion. Listening actively is an intellectual function; hearing is a biological function. Active listeners show they are listening through their facial expressions, body language, and comments. By repeating the other person's words and identifying their emotion, you demonstrate to them that you care about what they are saying. Paraphrasing the other person's message lets them determine whether or not you correctly interpreted their meaning.

To improve your listening skills, practice the following: (i) be motivated to listen actively by resolving that you want to listen well; (ii) be prepared to listen by learning all you can about the subject, the speaker and the situation and take notes when appropriate; (iii) be alert to all clues and hidden messages; (iv) think about what the speaker is saying as it is being said; (v) put yourself in the speaker's position and try to reach a mutual frame of reference; and (vi) ask probing and clarifying questions.

We listen through one of four primary styles; orientation to people, time, action or content.

"The way we communicate often has a direct influence on how we perceive and evaluate each other, and a vital element in productive communication is listening."

Women are more likely to be people oriented while men seem to be action, content or time oriented (Barker & Watson, 2000). If the average person speaks at a rate of about 125-175 words per minute and we can listen up to 450 words per minute (Carver, Johnson, & Friedman, 1970) it is no wonder communication is difficult, especially for those who listen to respond and not necessarily to understand. When the listener's mind gets ahead of the speaker, poor communication occurs.

Many studies have shown that effective leadership is tied to listening (Bechler & Johnson, 1995; Johnson & Bechler, 1998); leaders give good attention to

the speaker through eye contact (Orick, 2001); leaders paraphrase the person speaking to ensure an understanding of the message (Orick, 2002); leaders are able to relate accurately the message to another person (Orick, 2002); and leaders listen with an open mind and do not display emotion, defence or judgment (Orick, 2002). Listening is a skill many employers seek for entry level employees as well as those considered for promotion.

The problem is we are not taught how to listen in school, where reading and writing are primary concerns. The total daily average hours dedicated to communication activities are 1.82 for writing, 1.40 for reading, 4.83 for speaking, while listening accounts for 5.8 hours of the day (Janusik & Wolvin, 2006). Genuine listening is one of the few forms of competitive advantage.

Listen or thy tongue will keep thee deaf

The risk presented by poor listening and communication begins with weakened connections or relationships with others, often colleagues or team members upon whom we rely for goal attainment, success or merely satisfaction of being together. The way we communicate often has a direct influence on how we perceive and evaluate each other, and a vital element in productive communication is listening. The Chinese character for the complex verb 'to listen' is composed of the characters for the words ears, eyes, heart and undivided attention. Active listening is the gift we give those we need and like, expecting it to be reciprocated.

A primary characteristic of an effective listener is that of being attentive and showing genuine interest in what the speaker is saying. This can be accomplished by mirroring the body posture of the sender, either by positioning the body in a posture that is leaning forward in an open, accepting way, or sitting back in an attentive yet relaxed, reflective manner. Eye contact should be maintained with the speaker if it is not threatening and behaviours such as nodding the head and smiling will encourage the other person to continue. In addition, attempt to take mental notes of the sender's message; listen for the unstated message; ask mental questions that probe beyond the surface message; and concentrate on substance, not style. Effective listening through attentiveness, appreciation and validation is not achieved by taking turns talking but requires a concerted effort at mutual understanding. R&C

Tony Belak
Associate Director General
International Center for Compassionate Organizations (ICCO)
T: +1 (502) 413 2123 ext. 2
E: tony.belak@compassionate.center

PERSPECTIVES

THE 'DUAL-HAT' EXPERT – PUTTING ON AND TAKING OFF THE PRIVILEGED HAT

BY **STACEY A. BELL AND MELISSA L. KOSACK**
> BAKER & HOSTETLER LLP

The use of 'consulting' experts and 'testifying' experts can make or break a case. In modern-day commercial litigation, it is commonplace to have either one or both of these types of experts assist a litigation team develop case themes and strategy. By virtue of their skills, training, experience and education, these experts can (and often do) play a significant role in the outcome of a case. Among other things, they use their expertise to simplify complex facts – educating counsel, clients and triers-of-fact.

The role of consultant and that of testifier are often assumed to be separate roles played by different people. In fact, federal courts recognise this distinction between the two by according different rules, standards and protections to each with respect to discovery and confidentiality.

What happens, then, when the two get morphed into one – when the consultant becomes the testifying expert witness? What rules apply? What disclosure is required? Does a litigant forfeit the consultant privilege that would otherwise attach when that consultant is later proffered as a testifying expert witness? Or, as one federal judge colourfully phrased the question: "[W]hether, and to what extent, the work-product privilege applies when an expert alternately dons and doffs the privileged hat of a litigation consultant and the non-privileged hat of the testifying witness." *Yeda Research and*

Development Co., Ltd. v. Abbott GMBH & Co. KG (292 F.R.D. 97 (D.D.C. June 7, 2013)).

Unsurprisingly, as with just about everything else in complex commercial litigation, the short answer (to whether the privilege is waived when the two types of experts become one) is: it depends.

The privileged hat of the consulting expert

With the complexity of everyday transactions that form the basis of lawsuits nowadays – from the use of computers and electronic information systems to the globalisation of financial markets and international disputes over complicated securities transactions – the role of the consulting expert is critical in assisting counsel and clients better understand the factual and legal issues at play in a particular case.

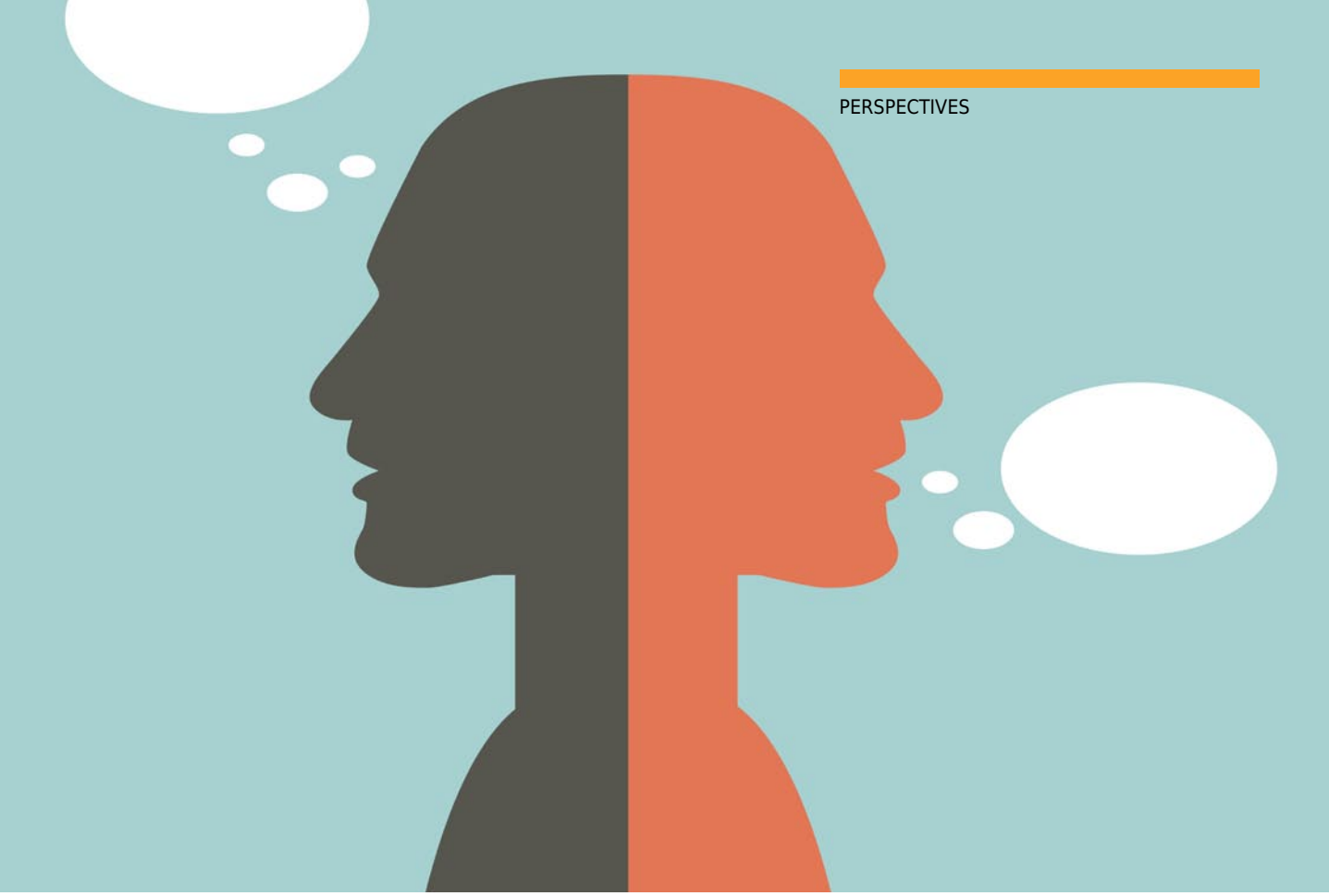
Consultants work alongside counsel in the development of case strategy – assisting with fact gathering and research, meeting with clients and key witnesses, and formulating legal strategy. As part of their role, consulting experts become intimately familiar with the strengths and, of course, the weaknesses of a given case.

For the consulting expert to provide the most value, counsel must be free to share their mental thoughts and processes without fear that an adversary may be able to discover those thoughts through their consultants. Because of this, federal courts recognise that communications between an attorney and a consulting expert are protected by the attorney-client privilege and/or the work-product doctrine. And, not only are attorney-consulting experts' communications protected, but consultants' work-product is protected in very much the same way as 'core work-product' of counsel (see Federal Rules of Civil Procedure, Rule 26(b)(4)(D) "a party may not, by interrogatories or deposition discover facts known or opinions held by a [] [consulting] expert.").

"The testifying expert has extensive disclosure requirements so that an adversary can test and probe the bases of any opinion that expert will offer at trial."

The non-privileged hat of the testifying expert

Unlike the consulting expert, the testifying expert has extensive disclosure requirements so that an adversary can test and probe the bases of any opinion that expert will offer at trial.



Of course, every case tells a story. Or, at least, two stories. Using scientific, technical or other specialised knowledge, the testifying expert plays a critical role in communicating one party's version of the story to the trier-of-fact. The expert witness is required to disclose all relevant information regarding the facts or data considered in connection with any opinions offered at trial. And, as determined by many courts, a testifying expert has 'considered' data or information if that expert has read or reviewed the materials before, or in connection with, formulating her opinions.

Though communications between the expert witness and counsel are accorded (limited) protection, this protection does not extend to information provided to the expert by counsel if the expert considered that information in forming the opinions to be offered in the case. Thus, unlike with consulting experts, providing privileged documents to a testifying expert waives any work-product protection previously afforded to those documents.

The dual-hat of the consultant-turn-testifier

As frequently happens during complex cases (because of time or budgetary constraints, or because of the intellectual capital that the consulting expert has already expended, among a

host of other reasons), the consulting expert who is protected from disclosure, and the testifying expert who is not, meld into one expert. What then are the disclosure requirements under these circumstances? What communications must be disclosed? What documents – either those received from counsel or those prepared by the expert – must be disclosed? Must they, for example, disclose any draft documents they prepared, particularly those identifying weaknesses in the case?

Though this area of the law is still evolving, a few principles have emerged out of cases tackling these questions: (i) once a consulting expert becomes a testifying expert, the scope of the attorney-client and privilege and work-product protection is typically narrowly construed; (ii) in dual-hat expert cases, the term considered is construed expansively in favour of the party seeking discovery; (iii) the privileged and non-privileged status of consultant and expert witness materials can be maintained only if the delineation between role as consultant and role as testifier is clearly made; (iv) to the extent that the delineation between the expert's roles as consultant and testifier becomes blurred, discovery will be allowed; and (v) the operative question in determining the discoverability of a document is not what hat the dual-hat expert was wearing at the time of the creation of the document, but whether this expert considered the document in connection with the opinions in the case.

At bottom, courts will apply the broader discovery for testifying experts to everything except materials generated or considered uniquely in the expert's role as consultant. It bears noting that courts will not necessarily rely on the dual-hat expert's determination of which documents she considered solely in her testifying capacity; the court may request an in camera inspection of the privileged and non-privileged documents at issue, regardless of which hat she claims she had been wearing.

Best practices for working with dual-hat experts

Ideally, it is best to maintain the separation of roles between these two types of experts. However, converting your consultant into a testifier might be the most practical approach, so, if your expert must 'don' and 'doff' the privileged hat, below are some things to keep in mind.

Define the expert's role. Determine which hat your expert will be wearing for which task as early as possible in the litigation. Evaluate whether the issues and corresponding documents are so intertwined that the expert will need to interchangeably put on and take off the privileged and non-privileged hats. In such a situation, operating under the assumption that all documents provided to the dual-hat expert are at risk for disclosure is the prudent practice.

Create a new retention letter. Enter into a new retention letter if switching from consultant to expert witness. This will create a temporal line in the sand

(as an aside, experts operating in either capacity, should be retained by outside counsel – not by the client – in order to preserve the protections afforded by the attorney-client privilege and/or the work-product doctrine).

Share sparingly. Given the litigation trend of resolving any ambiguities concerning dual-hat discovery disputes in favour of parties seeking discovery, parties should be very careful about disclosing core attorney work-product to dual-hat experts. If case considerations advocate disclosure, make sure that the dual-hat expert will not need to consider, review or analyse the document while wearing her testifying expert hat or that you have performed a cost-benefit analysis and are comfortable with disclosure.

Clearly delineate subject matter. Clearly identify the subject matter requiring opinion testimony. Ask the dual-hat expert to treat the consulting and testifying work as two separate engagements by maintaining and tracking documents separately, restricting communications with counsel by task codes, and determining the specific analyses and conclusions underlying each of the two assignments.

Prepare for discovery battles. The contours of what discovery is required from a dual-hat expert are still evolving. Be prepared for discovery disputes and motion practice around issues pertaining to the contours of the attorney-client privilege and the work-product doctrine. R&C

Stacey A. Bell
Partner
Baker & Hostetler LLP
T: +1 (212) 589 4632
E: sbell@bakerlaw.com

Melissa L. Kosack
Counsel
Baker & Hostetler LLP
T: +1 (212) 589 4274
E: mkosack@bakerlaw.com

PERSPECTIVES

CHEMICALS IN COMMERCE: THE IMPACT OF TSCA SAFETY REFORM

BY **JULIE BYRNE AND BARRY MCLAUGHLIN**
> 3E COMPANY

While largely seen as a boon for public health and environmental protection, the federal Toxic Substances Control Act (TSCA) has proven at times to be a restrictive reality for the chemical industry. The legislation, enacted in 1976, remains the nation's primary law for chemicals management and calls for an inventory of all chemical substances manufactured, processed or imported into the United States. As a result, the US Environmental Protection Agency (EPA) has been tasked with testing chemicals and maintaining an ever-enlarging inventory of 85,000 chemicals, up from the 62,000 chemicals monitored at the law's inception.

In a major overhaul of federal chemical safety laws, a historic reform of TSCA took effect on 22 June 2016. The Frank R. Lautenberg Chemical Safety for the 21st Century Act is intended to provide the EPA with better tools to obtain testing information on chemical substances. It also eliminates certain statutory requirements that make the restriction or ban of chemicals in US commerce difficult, restructuring the way existing chemicals are evaluated and regulated by directing the agency to use scientific evaluation to guide its decisions.

Before the passage of the TSCA reform, the EPA was unable to restrict or ban a chemical's use – or even request new toxicity data from its manufacturers – without first proving the chemical

carried a certain level of risk to human health or the environment. The EPA was also required to look into the potential costs of regulating a chemical when determining whether it was safe for use and choose the "least burdensome" method of regulation. Those requirements severely limited the EPA's ability to take action under TSCA.

EPA authority: a stronger hand

Going forward, the EPA will no longer have to satisfy cost-related requirements for regulation and will wield more authority to restrict or ban chemicals or require companies to submit new toxicity data. Federal law now directs the EPA to review the safety of chemicals determined by the agency to be a high priority. It also establishes a standard for prioritising chemicals that accumulate in the human body, do not break down easily in the environment, or are already known to be highly toxic.

Among its reforms, the revised law is intended to do the following: (i) create a system for risk-based safety evaluation for existing chemicals, based on scientific standards; (ii) require the EPA to evaluate risks of existing chemicals under "judicially enforceable deadlines", without consideration of cost; (iii) set deadlines for the EPA to take certain actions, such as an affirmative safety finding within a 90-day pre-manufacture notice (PMN) review period and completion of risk assessments within three years of enactment; (iv) reset the TSCA inventory by identifying active and inactive chemicals on the market; (v) require the EPA to designate low and high priorities of chemicals, conduct risk evaluation of high-priority substances, and restrict or ban those that present an unreasonable risk; (vi) eliminate the "least burdensome" requirements for regulating chemicals; (vii) initiate a review of all existing confidential business information (CBI) claims and require re-substantiation of approved claims after 10 years (the legislation also allows certain state, local, and tribal government officials and healthcare professionals to access the information); (viii) provide federal pre-emption of state law with certain waivers; (ix) require identification and protection of the most vulnerable populations, such as children, pregnant women and chemical workers; (x) advocate non-animal testing, such as quantitative structure-activity relationships (QSAR); (xi) require science-based decisions, founded on weight of evidence (WoE); and (xii) allow user fees to be collected and used directly for the EPA's chemical management activity.

TSCA timelines

In accordance with the 22 June enactment of the law, the following timelines are taking effect, requiring near-term action from the EPA. The EPA must develop a plan for implementation within six months, develop new policies and guidance within two years, develop guidance within one year for draft risk evaluations, publish the schedule of risk evaluations each year, and establish a Science

Advisory Board to act as independent advisers on TSCA reform within six months.

TSCA reform law has wide-ranging impacts on industry. Highlighted below are some of the new requirements for both the EPA and companies involved in the manufacture, processing, use and disposal of chemicals in the US.

Regulatory changes

In TSCA Section 4 the EPA has increased authority to require testing of chemicals (existing or new) as part of the risk evaluation process. The EPA must publish its scientific rationale for any testing requirements. The testing requirements must minimise animal testing. The EPA must also work to develop non-animal testing protocols. Any testing requirements must be in a tier-based approach unless there is scientific proof that would show that higher-level testing is required.

Under TSCA Section 5 the EPA must review all PMNs within the required 90 days, with only an additional 90 days allowed. If a PMN or Significant New Use Notice (SNUN) is not reviewed within 180 days, any submission fees will be refunded. The EPA must issue a determination as part of the review of a PMN or SNUN. As part of the determination, the EPA must make an affirmative finding about the level of risk posed without regard to costs.

As per TSCA Section 6, the EPA must generate a list of high-priority and low-priority chemicals to undergo full safety assessment and risk evaluation.

The first 10 chemicals will come from the 2014 work plan. Within three and a half years, at least 20 high-priority chemicals must be in the process of being reviewed and 20 low-priority chemicals identified to be reviewed. The EPA will be required to publish the annual list of chemicals to be reviewed.

All risk evaluations will be required to be completed in three years and published for public review. The risk evaluations will include a review of hazards and exposures. Cost will not be allowed as a consideration in any proposed testing. The EPA will be allowed to require manufacturers and importers of evaluated chemicals to pay for the risk evaluations. The industry will also be able to nominate chemicals to be added to the list; the nominator of chemicals added to the list will be required to pay for the risk evaluation.

TSCA Section 8 dictates that the EPA will require industry to provide a list of all active chemicals manufactured, processed or imported in the previous 10 years. This information will be used to reset the TSCA 8(b) inventory list. Chemicals not included on the reset TSCA 8(b) inventory list will require a notification to be submitted before commercial use.

Under TSCA Section 14, as part of TSCA reform, the EPA will review all claims of confidential business information (CBI). Any claims of CBI will require substantiation from the submitter and will require resubstantiation every 10 years. The EPA will now be able to release CBI in some instances to certain state, local and tribal government officials and healthcare professionals. For cases where a chemical receives an unreasonable risk determination, a CBI claim will be denied.

"All risk evaluations will be required to be completed in three years and published for public review."

In TSCA Section 18 under the new legislation, the federal government will be provided with pre-emption of state law with certain waivers. States may not enforce any restrictions imposed after 22 April 2016. State laws in place before 31 August 2003 (that is, California Proposition 65), will still be valid. Once the EPA finishes an evaluation on a chemical, states cannot add additional restrictions.

TSCA Section 26 establishes that under the new law, the EPA's budget will never be lower than 2014 levels. The EPA will be allowed to collect up to $25m

annually in fees. The fees for PMNs and SNUNs will no longer be capped at $2500, although the lower fees for small manufacturers remain in place. All of the fees collected will be deposited into the EPA's account.

TSCA reform will likely have significant impacts on chemical manufacturers, importers, distributors, processors and other downstream users. Nearly every company involved in the chemical industry doing business in the US is affected by TSCA regulations to some degree, with various exceptions among food, drug, cosmetic, nuclear and pesticide companies. Raw materials, intermediates, finished goods and some articles are all regulated by TSCA. Full life-cycle, cradle-to-grave compliance is an essential component of TSCA, as most manufacturing, importing, processing and disposal activities are regulated under TSCA.

Penalties for non-compliance can include civil litigation and monetary settlements, criminal prosecution, fines and damage to a company's brand or reputation – as well as the potential negative impact on a company's ability to do business. Wilful violators can face imprisonment.

Increased TSCA requirements resulting from the EPA's chemical management reform as mandated by the TSCA reform bill and increased enforcement should only accelerate the burden on organisational environmental health and safety (EH&S) compliance activities. By developing and maintaining a comprehensive and forward-looking plan for compliance, companies can better prepare for the inevitable. R&C

Julie Byrne
Chemical Regulatory Consultant
3E Company
T: +1 (760) 602 8746
E: jbyrne@3ecompany.com

Barry McLaughlin
Authoring Project Manager/TSCA Specialist
3E Company
T: +1 (760) 476 8908
E: bmclaughlin@3ecompany.com

PERSPECTIVES

CONSUMER PRODUCTS INDUSTRY SECTOR – FRAUD, AREAS OF RISK AND HOW TO MITIGATE THEM

BY **OLAOLUWA DADA**
> ERNST & YOUNG

The Fast Moving Consumer Goods (FMCG) industry is a fertile area for fraud. FMCGs are products that are sold quickly and at some point, at considerable prices. By nature, FMCGs are of a short life span. They are either durable, such as kitchen utensils, which are eventually replaced over a period of time, or non-durable, such as processed foods, soft drinks, etc.

Due to the fast moving structure of the products, there is a high risk of fraud. For example, salespeople have to meet their targets, potentially giving rise to numerous fraud occurrences.

Litigation involving consumer fraud is always met with a high fine, and ultimately reputational damage. Because of the nature of the business characterised by quick sales, they are always a breeding ground for fraud.

What are these areas of risks, and how can they be identified?

In the consumer industry sector, there are red flags to identify when checking for fraud. If there is no proper control over the inventory management, companies could lose huge amounts of money in

physical cash and assets to fraud. It is important to conduct a regular, surprise check/count to test for accuracy. Compare the perpetual inventory to the physical records and identify any exceptions. If this does not add up, there could be cases of inventory shrinkage. It is worth noting that surprise counts should be carried out on any personnel, including the warehouse manager or store keeper, as the case may be. The reason for this is to allow objectivity and independence in the exercise.

In addition to the checks, there are inventories that are written off as scraps or inventories that have, say, expired and are consigned to be destroyed. There should be appropriate oversight over the discarding of such materials, such as approval from top level employees, and also a certificate of destruction.

Third party activities. Third parties, such as distributors, agents, vendors, etc., may act in an unethical manner on behalf of clients, which may ultimately create liability for the client. This liability could be in the form of reputational damage or litigation settlement, for example. There should be adequate third-party oversight in place. Areas of risk to consider with respect to third parties include

testing to identify whether there is a contract with the third party, reviewing records detailing whether third parties have been trained on the company's anti-bribery and anticorruption policies, and testing whether appropriate due diligence has been performed and documented on the third party. In the event the third party is a high risk, or operates in a volatile economic environment, it is important to review records to determine whether a proper background check has been conducted for the vendors.

Falsification of sales documents. Falsified sales documents could be tendered for either immediate or long-term satisfaction. False or altered documents can serve as the basis for overstating revenue, which will conclusively reflect on the company's financials. Areas of risks include testing to ascertain whether the documents were adequately approved, testing to see whether they reflect actual expenses, and ascertaining whether supporting documents are available.

Non-disclosure or partial disclosure of sales. Sales could be made with either part or none of the actual transaction being recorded. Are there side agreements that imply unaccounted-for rights? Are there issues of 'channel stuffing' that could result in improper revenue recognition?

Segregation of duties. Although the song on segregation of duties is sung by many organisations, only a few implement this control strategy. Segregation of duties can not only unravel the mystery around transactions, it can also assist in identifying the persons involved. Areas of risk to consider with respect to segregation of duties include testing to see if the person in charge of accounts payable is the same as the person in charge of account receivable, and reviewing the approval structure of the organisation. For example, when it comes to the purchasing or the distribution of goods or product, is just one person charged with this responsibility, or does it require the involvement of multiple persons? When an organisation has a culture of segregation of duties, it is harder for fraud to occur, and much harder for it to go unnoticed.

> **"Fraud cannot be completely eradicated, but it can be adequately mitigated."**

Knowledge of code of conduct. A common mantra is 'knowledge is power'. One can only act on what one knows. It is a risk if employees are not aware of the company's code of conduct and the code

of ethics. Adequate training should be given to everyone. A well-informed employee will save the company many problems when it comes to dealing with fraud, because they are aware of the process.

In addition, it is important for each organisation to set up an enterprise risk management (ERM) process. An ERM process is a framework (typically electronic) that contains information on the different risks faced by an organisation. The purpose of the ERM process is to be able to efficiently identify and assess the risks faced by an organisation. These are risks that may have negative impacts on an organisation. Once these risks have been identified and assessed, the ERM process helps to tackle or mitigate the risks, as the case may be.

With an effective ERM process in place, an organisation can adequately address risks, such as categorising them appropriately, i.e. as high, medium or low risk.

When identifying and assessing these risks, it is important to secure the attention of employees who are knowledgeable in those areas. From a general point of view, this should include the chief compliance officer, the chief risk officer, the general counsel or attorney/legal director, as well as the chief financial officer and the chief executive.

In certain cases, the process for managing these risks should be also present in the ERM process.

Although this is not an exclusive list of all possible fraud risks in the consumer industry, it does help to point out to compliance and integrity functions where fraud risks might emanate. Fraud cannot be completely eradicated, but it can be adequately mitigated. R&C

Olaoluwa Dada
Forensic Analyst
Ernst & Young
T: +23 480 66 469 775
E: olaoluwa.dada@ng.ey.com

PERSPECTIVES

LIABILITY FOR 'MADE IN USA' CLAIMS

BY **LESLIE T. KRASNY**
> KELLER & HECKMAN LLP

In the US, challenges to 'Made in USA' and other US origin claims, brought under both federal and state laws, have increased in recent years. Some companies mistakenly believe that a claim of US origin is automatically permissible if a product does not need to be marked with a foreign country of origin pursuant to Tariff Act regulations, but such claims must also meet criteria regarding foreign content and processing.

There is no requirement to disclose the US origin or the amount of US content for most products marketed in the US. A voluntary statement regarding US origin or content may be made, however, if a product meets the Federal Trade Commission (FTC) guidelines on Made in USA claims. The FTC policy applies to claims in labelling and advertising, including marketing by means of internet or email.

Under the FTC policy, unqualified US origin claims may not be made unless the product is "all or virtually all" made in the US. This means that all significant components and processing must be of US origin (with no, or negligible, foreign content). To determine the amount of US content, marketers should determine whether there is any "significant" foreign content, which involves knowing the point at which foreign content was incorporated and whether it is a direct part of the finished product.

The FTC policy also allows qualified Made in USA claims, for products that do not meet the criteria for unqualified claims, if there is significant US content

or processing. The claims would have to communicate the nature of the domestic connection, such as "manufactured in the US from domestic and foreign ingredients". But even qualified claims may be violative if there are misleading implications regarding the amount of domestic content or the extent of domestic processing.

On the state level, only California has a law covering Made in USA claims. Until January 2016, the California law was more restrictive than the FTC standard, prohibiting unqualified Made in USA claims if any part of a product was produced outside the US. Thus, even if a company had adequate substantiation to support a claim under the FTC standard, there might have been a violation of California law.

Under the new California standard, products bearing Made in USA claims generally may contain up to 5 percent foreign content (measured as a percentage of the final wholesale value of the product). And products may contain up to 10 percent foreign content if the manufacturer can demonstrate that the foreign-sourced components could not be produced within the US.

The new California law is similar to the FTC policy, but there are important differences. Unlike California law, the FTC standard does not contain maximum percentages for allowable foreign content, and applies subjective criteria including the likely significance to consumers of the amount of any foreign content. Moreover, California expressly addresses only unqualified Made in USA claims. And the scope of the FTC policy is broad, applying to all marketing materials, whereas the California law applies just to Made in USA label claims.

A recent trend is the filing of putative class action lawsuits, by private plaintiffs, for false or misleading Made in USA or other US origin claims under state consumer protection laws. In May 2016, for example, a putative class action lawsuit was filed against a dietary supplement manufacturer, in federal court in Illinois. A number of state consumer protection laws provide that consideration must be given to the interpretations of the FTC concerning unfair or deceptive trade practices. The lawsuit alleged that particular vitamin supplements labelled as Made in the USA do not comply with the "all or virtually all"

FTC policy because the products contain foreign-sourced ingredients which constitute a "significant part" of the products.

To help support the allegation of consumer reliance on the Made in USA claim, the complaint cited a 2015 survey by Consumer Reports magazine which found that nearly 80 percent of Americans are willing to pay more for American-made goods. The lawsuit seeks injunctive relief, actual damages to consumers in nine states (calculated by the difference in price between the product as sold and what it would have been worth had the products not been deceptively advertised), punitive damages and attorneys' fees.

In addition to the risk of class action lawsuits, companies making Made in USA claims are subject to enforcement action by the FTC. Companies being investigated for making deceptive Made in USA claims may be able to resolve a case informally with the FTC by agreeing to a remedial action plan that uses qualified claims to communicate the extent of US components or operations without deceiving consumers, including prominent placement of approved qualified claims on revised packaging and in-store displays, as well as information on the company's website and social media pages.

There can be investigations by state Attorneys General too. In October 2015, the Texas Attorney General settled a case regarding Made in the USA claims on the labels of solar panels made in China, which were alleged to violate the Texas Deceptive Trade Practices Consumer Protection Act. The company agreed to a resolution that could cost $5m in civil penalties and $2.8m in restitution for customers, although the exact amount of the payments will depend on the company's bankruptcy proceedings.

"Companies should ensure that there is a basis for making Made in USA claims, by having competent and reliable evidence substantiating the FTC and California criteria, at the time the claim is made."

There is also potential liability under the federal Lanham Act, which authorises litigation between competitors based on marketing claims. A marketer can be held liable for any claim that misrepresents the nature, characteristics, qualities or geographic origins of its goods. Violations of the Lanham Act may subject a company to injunctive relief,

disgorgement of profits, a damage award to a competitor of up to three times the damages and attorneys' fees.

Companies should ensure that there is a basis for making Made in USA claims, by having competent and reliable evidence substantiating the FTC and California criteria, at the time the claim is made. The FTC takes the position that marketers can rely, in good faith, on information from suppliers about US domestic content. In order to establish adequate substantiation in the event of a challenge, the information from suppliers should be in writing, and preferably in the form of a certification as to the minimum percentage of US content. R&C

Leslie T. Krasny
Partner
Keller & Heckman LLP
T: +1 (415) 948 2810
E: krasny@khlaw.com

HOT TOPIC

DEVELOPING AND MANAGING AN EFFECTIVE INTERNATIONAL TRADE COMPLIANCE PROGAMME

PANEL EXPERTS

Darko Neuschul
Manager of Customs and Global Trade
Facebook Inc
T: +1 (415) 290 9788
E: neuschul@fb.com

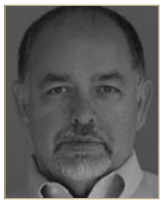
Darko Neuschul is the manager of customs and global trade at Facebook Inc. Before Facebook, Mr Neuschul was a senior manager in the San Francisco office of Ernst & Young's customs and international trade practice. Before returning to Ernst & Young in 2011, he was a senior manager in Deloitte's customs practice and a manager in Deloitte's Central European indirect tax practice, and was also leading the tax function of Deloitte in Sarajevo, Bosnia. He is a customs and global trade specialist with 17 years of experience in customs compliance and international trade.

Michael Cone
Partner
FisherBroyles
T: +1 (212) 655 5471
E: mcone@fisherbroyles.com

Michael Cone concentrates his practice in the areas of administrative, customs and international trade law. He counsels clients on a wide array of regulatory compliance issues, with administrative expertise that includes matters falling under the jurisdiction of US Customs and Border Protection (CBP) and the panoply of other administrative bodies that regulate the importation, exportation, marketing and sale of merchandise.

Agnes Cruz
Head of Customs
Nokia
T: +55 (11) 95742 5532
E: agnes.cruz@nokia.com

Agnes Cruz is an international trade professional with 22 years international experience in customs compliance. She has worked in the telecoms industry for 16 years, the last nine of which as head of customs. Ms Cruz focuses on customs valuation and classification, country of origin, Incoterms, free trade agreements and customs compliance matters, involved in the global movement of goods among 120 countries.



Marshall Smith
customs manager
Starbucks Coffee Company
T: +1 (206) 318 4885
E: marsmith@starbucks.com

Marshall Smith is a customs manager with Starbucks Coffee Company in Seattle, Washington. He has over 30 years of experience in management including over 20 years in international shipping. His career has included such diverse industries as customs compliance, importing and exporting, cargo security, oil & gas drilling, industrial sales, television retailing, customer service and real estate.

RC: Could you provide a general insight into the complex array of trade regulations with which companies engaged in global trade have to contend?

Cone: Multinationals face a daunting panoply of regulations in every country where they do business. Take the US. Aside from basic customs rules on classification, valuation and country of origin, Customs and Border Protection (CBP) helps enforce the regulations of over 40 other federal agencies possessing an interest in imported goods. For example, imported food, cosmetics and drugs must comply with regulatory requirements of the Food and Drug Administration, children's items are subject to safety standards promulgated by the Consumer Product Safety Commission and vehicles parts must comply with standards of the National Highway Traffic Safety Administration. For goods moving out of a country, export control regimes can be highly complex and often bifurcate strictly controlled 'things that go boom' with more easily traded silent merchandise. There are also anti-bribery regimes to fight corruption and sanctions regimes combating business with unsavoury characters, both of which have extraterritorial grasp. It is a complicated and risky landscape.

Smith: Complexity is driven by factors such as geography, political agendas, protectionism, products, safety, security and communication, just to name a few. Fortunately, there are some consistencies in global trade that provide a degree of regulatory certainty, such as trading with a member nation of the World Trade Organisation (WTO), or the general consensus among developed nations involving anticorruption, although this is still evolving. Beyond that, products and services moving across borders are subject to a multitude of import and export regulations that are product specific. For instance, a food product may be subject to numerous regulations from multiple agencies such as customs, agriculture and food & drugs in both the country of export and their equivalents in the country of import. Remaining current with regulatory changes, interpreting both the spirit and letter of the requirements – often in multiple languages – and communicating these requirements effectively to an internal audience are some of the key challenges faced by today's global traders.

Neuschul: Trade regulations, and their impact, are a key driver for a business' planning, decision making and execution processes when entering a new market or when facing trade regulation changes in an existing one. To highlight the complexity of such regulation, let us just look at what goes on with one single transaction from the US. When the transaction is initiated, contracting involves applying Incoterms, performing anti-boycott and sanctions screening and export controls considerations – such as ECCN,

deemed exports, dual-use, government users, and so on. Upon export, filing and recordkeeping rules apply. Once the goods arrive at their destination, a customs declaration containing correct classification, country of origin, value and other information has to be filed, and in order to do that, we must have a registered importer of record, a customs broker and a trade compliance programme that will monitor and manage all these risks. Hence, viewed on this most basic level, one can see how complex the global trade-regulatory environment can be for a truly global company.

Cruz: The primary regulators in the field of customs are two intergovernmental organisations: the WTO and the World Customs Organisation (WCO). The implementation and interpretation of the legal instruments issued by these bodies vary depending on the area, region and country. Each country controls customs compliance based on national regulations. The WTO regulates multilateral trade issues including general duty levels, non-preferential country of origin, abolition of non-tariff barriers, trade dispute settlement and the ITA Information Technology Agreement. The WCO regulates multilateral customs issues including the harmonised tariff code and the valuation of goods for customs purposes. Free trade and duty agreements – such as EUR-MED, NAFTA or MERCOSUR – regulate bilateral and internal duty levels between members, as well as preferential country of origin. There are also country-specific rules and regulations, national boards of customs of individual states and the International Chamber of Commerce (ICC) to consider.

> **"Multinationals face a daunting panoply of regulations in every country where they do business."**
>
> *Michael Cone, FisherBroyles*

RC: What are the main legal and regulatory developments to have impacted international trade over the past 12 months? What steps can companies take to monitor changes and update their compliance programmes?

Cruz: The recent economic situation has brought several bilateral agreement changes, some to an almost unreachable level of compliance criteria. Origin restrictions due to political reasons have also been a challenge. A vicious circle of economic

challenges has also made the component and manufacturing industries move their factories constantly or have multiple locations producing the same goods. It is critical to have control of your supply environment, since the most visible impact is usually a bottleneck at the moment of exporting and importing. Origin sourcing criteria can and should be implemented either via frequent training or regulation of procurement and product development organisations. It is also recommended to monitor supplier origin declarations and exert control over the end-to-end flow.

Neuschul: The main recent regulatory developments relating to international trade globally have been in the area of export controls. In addition to the US Export Control Reform initiative, which has recently seen many amendments to specific rules and regulations, there is a whole list of countries which are either initiating or upgrading their export control legislations. A company dealing with controlled products, technologies or software can be profoundly impacted by these reforms, and monitoring this impact is crucial. It is important to understand what 'controlled' means. Usually, it is a paramount task for any given company's trade compliance function to do this monitoring on its own on a global scale. Hence, it is advisable to have either appropriate involvement with industry groups, which have bodies that monitor and inform their members, or have counsel that can keep the business well informed and helps with planning on how to address these changes.

Smith: In the US and Europe, it could be said that changes in their economic sanctions postures over the last year could have presented the biggest challenges for global traders. Additionally, there has been a pronounced uptick in more aggressive enforcement, specifically in the area of anticorruption. Traders also have to plan for anticipated changes in the regulatory landscape resulting from the next generation of trade agreements that go beyond the traditional duty preference model and now include provisions for human rights and the environment. For companies with a complex supply chain, these changes can

> **" It is critical to have control of your supply environment, since the most visible impact is usually a bottleneck at the moment of exporting and importing."**
>
> *Agnes Cru, Nokia*

take years to plan for and implement. Monitoring regulatory changes on a global scale and keeping a compliance programme up to date require both a solid network of external service providers and internal stakeholders, regionally and locally.

Cone: The past 12 months have been marked by substantial uncertainty. The TPP and TTIP now appear destined for the political graveyard but the impact of Brexit on trade flows and investment remains unclear. There has been increased enforcement on both sides of the Atlantic in the areas of export controls, anti-bribery, customs and banking regulations. A new trade and investment regime in Brazil, the *Trek Leather* court decision in the US which broadened the domain of companies and individuals potentially liable for customs violations, and new regimes for the enforcement of intellectual property and antidumping laws in the US, will impact many multinationals. Companies need to pay close attention to developments to ensure that revisions which affect their core areas of trade do not interrupt the movement of goods through their supply chain or disrupt their operations due to concomitant enforcement actions.

RC: Developments such as Brexit, the stalled TPP and TTIP, and the failed Doha round all point to a retraction from free trade by world populations and governments, and an increase in barriers to trade. How will these trends impact multinational companies, and how can they adapt given the uncertain future of global free trade?

Neuschul: These developments not only present uncertainty in terms of global free trade, but can be crucial to a company's future in certain markets overall. Issues such as tax treatment, global expat positioning, capital liquidity and security and revenue/profit repatriation are all impacted. The global trade planning and compliance function plays only one part in this process, but it is a very important part. The reason it is usually important, among the more obvious things, is that it is on the operational forefront and can shed light on other crucial potential issues. As companies plan for these legislative and political movements, it is imperative that the resources that the company has for managing the global trade function have a seat at the big table where existential decisions about the company's future are made.

Cone: Recent global developments, including Brexit and the stalled global trade talks, reflect the growing suspicion on the part of populations in the industrialised countries that the free trade deals of the past have not worked to their benefit. Multinationals, who have benefited most from free trade deals, should consider revising supply

chain strategies to increase local content and local employment, while decreasing their energy and pollution footprint. Such adaptations may help shift public opinion in favour of multinationals' products. Increased use of local branding, rather than pursuit of worldwide branding, may also help shift local perceptions. By increasing production in G-7 countries and making it well known, multinationals can increase consumer mindshare among critical populations.

Cruz: It is uncertain whether the EU and the US, having driven a global trade liberalisation agenda in the past, will remain equally engaged in global trade policy in the future. Hence, the international trade regime of the WTO and its multilateral approach should be valued. Bilateral FTAs are good when global agreements fail; however, a grid of FTAs will not replace a global solution because of complex and more globalised supply chains.

RC: How important is it for companies to efficiently and strategically integrate import and export processes into their overall business plans and supply chain management procedures? What are some of the common challenges in achieving this goal?

Smith: A global trader that has not fully integrated its import/export strategy into its business plan will not remain competitive. Many companies rely heavily on strategic global sourcing to maintain their competitive advantage. Margins can be significantly impacted by duty management, such as the use of free trade agreements. Supply chains can realise greater efficiencies and lower landed costs through the strategic use of free trade zones and trusted trader partnership programmes that can reduce dwell times thus increasing velocity. The challenge for most companies begins with hiring talent with a strategic perspective. Many companies start out with a domestic focus and later evolve internationally. The import/export functions in these companies tend to follow the same path, never fully developing the strategic expertise required for a successful global trader. Next, the challenge is to position that expertise organisationally so that it has a seat at the strategic planning table, so to speak.

Cone: Lean manufacturing requires real-time visibility into import streams. Where lean manufacturing is not matched with pending orders, reduced inventory costs are not achieved. Thus, manufacturing companies sourcing imports from abroad and exporting finished products face substantial challenges to maintain visibility into both the import and export streams of their operations, manage local and international freight, adjust to input shortages and cancelled purchase orders, and communicate effectively with all their business partners. Software plays a crucial role in

supply chain management, but companies must also establish effective internal controls so that internal divisions such as purchasing, warehousing, logistics and accounting keep each other appraised of key developments and contingencies. A common problem affecting multinationals is parental control over sourcing, invoicing and payments. Lack of local autonomy can result in higher costs for inputs and third-party services as well as a subsidiary whose management personnel feel disenfranchised.

Cruz: It is important to safeguard risk management, overall process compliance and seamless execution, using proper ERP systems that support regulatory updates on the implemented environment. Challenges start with understanding the importance and split of customs clearance procedures as part of the entire supply chain, bringing different legal aspects to be addressed beyond just cost efficiency. Related questions might include, "What is the business case to implement a risk mitigation action?" and "Does the investment pays out?" Furthermore, the question should be different when it comes to the legal impact on compliance, such as: "What could be the impact on our business if a non-compliant operation is performed systematically?"

Neuschul: I believe that most, if not all, successful supply chain management professionals understand the need for well functioning global import/export processes. However, as we look at other areas of the business, which are impacted by export and import related legislation, such an understanding might not be so obvious. To illustrate, for example, a company developing certain technology or software might employ nationals of multiple countries, and have code and design repositories open to all or most employees. This so called 'deemed exports' area can be easily overlooked, as HR might not be the traditional collaborator of the global trade function, and violations can be significant. One way to address this effectively is to have the trade function empowered enough to have insight into areas outside of just supply chain. Having trade as part of an operational yet central function, such as tax, is a way to provide that insight.

RC: In your opinion, how difficult is it for multinational companies to navigate the complex area of Free Trade Agreements (FTAs)? How should companies go about managing FTA requirements such as acquiring a sound understanding of rules of origin, for example?

Cruz: In the last five years, the number of FTAs has almost doubled, transforming opportunities into challenges for companies working in a global environment. Therefore, it is recommended that companies have access to a specialist in this area acting on it as a predominant task, or, depending on

the size of the operation, a dedicated organisation that can establish company-wide coverage and a good governance programme. Last but not least, companies should get support from professional tools, where all FTA-specific rules are updated by a single source.

Neuschul: For some companies, FTAs and other duty relief programmes have huge cost impacts. However, before a duty relief programme is implemented, we need to know with certainty how big such savings are, and present to management that these savings are material to the organisation and that the savings exceed the costs of administering such programmes – metrics, metrics and metrics. One good thing is that many new and existing FTAs are modelled after similar rules, hence making the origin determination and recordkeeping processes more streamlined across multiple FTAs. The compliance management for FTAs is more involved and requires a higher degree of diligence compared to other trade processes. Ultimately, duty relief programmes have to be approached with caution and the full understanding of both costs and benefits needs to exist before a programme is implemented. Having a good internal audit control measure that monitors compliance is money well spent.

Cone: FTAs present enormous trade advantages for scrupulous companies. Unfortunately, they contain a variety of pitfalls arising not only from excruciatingly complex rules of origin but also from gaps in specificity and interpretation that are often worked out only in adversarial proceedings with the importing company on the defensive. When disputes arise the stakes are always high as FTAs either eliminate or drastically reduce customs duties. The opportunity for significant duty savings means FTAs lend themselves to abuse and are considered high risk by customs authorities. Along with antidumping and countervailing duties, IP infringement and textiles and wearing apparel, CBP considers FTAs as a 'Priority Trade Issue' because they "represent high-risk areas that can cause significant revenue loss and harm the US economy". Administrative and court actions frequently arise over FTA claims and

> **"Duty relief programmes have to be approached with caution and the full understanding of both costs and benefits needs to exist before a programme is implemented."**
>
> *Darko Neuschul, Facebook Inc*

multinationals should consult with expert customs counsel prior to claiming FTA preferences.

Smith: FTAs can be very difficult to manage. Some companies with a narrow product mix or simple bill of materials can manage without too much difficulty, but others who manage numerous products with a complex bill of materials and origins requires entire departments of experts who ensure the accuracy of their preferential claims. Confounding the process even further is the volume of FTAs on a global scale, each with their specific rules, and the process of qualifying a claim which requires clear communication and cooperation from the supplier base. To effectively manage an FTA programme, a focus must be applied to compliance with the terms of the agreement. Preferential duty claims are a perennial area for audits. Internal controls should be maintained, such as recordkeeping, training, auditing and the monitoring of programme changes, among others. Traders need to do a risk assessment and develop a sound business case for the use of FTAs.

RC: What are some of the penalties that companies might face if they are found to be in breach of international trade rules and regulations?

Cone: Companies fall into trouble for import violations, export violations, overseas bribery, doing business with an entity on the 'bad guy' sanctions list, and various other regulatory missteps. On the import side, CBP will seek to collect any customs duties it thinks went unpaid and then often attempt to penalise the importer for between two and four times the unpaid duties as icing on the cake. Where another agency's regulations are at issue, CBP will seize the imported merchandise while the sister agency brings a parallel administrative enforcement action. Penalties for export control violations, overseas bribery and sanctions violations can be astonishingly severe, routinely in the millions of dollars. Each agency has its own enforcement regime, regulations and personality, so effectively responding requires skill. Unfortunately, when agency

> **"While financial penalties are effective in driving behaviour if they are large enough, the most concerning penalty for a high volume global trader is the possibility of debarment."**
>
> *Marshall Smith, Starbucks Coffee Company*

enforcement actions do arise, the cost of defending them and paying any fines imposed quite often exceeds the value of the goods themselves.

Neuschul: The penalties are as varied as are the ways in which a company can violate various rules and regulations. The financial penalties can be quite draconic – and surprising – in some cases. A common misconception is that if a good is imported duty free into a country, the risk of penalties must be low as well. Violations do not have to result in a loss of revenue for a government in order to be financially high. In case of import violations, the penalties are usually assessed as a percentage of value of the goods, or as a percentage of the VAT that was payable on such imports. When compounded over time and with penalty interest, and given they are not tax deductible either, the amounts add up quickly. On the other hand, with export controls related violations, the penalties can also add a business and reputation risk dimension, where a business loses its export privileges.

Cruz: Non-compliance with customs and export control regulations may expose the company to financial risk, such as tax and customs fines, which are mostly calculated as a percentage over the violation transaction amount, administrative offences and failures in customs audits. There may also be business disruption, including reviews of permits and licences, loss and or discontinuation of agreements, transactions investigation and further audits.

Smith: The obvious penalties are monetary, which, depending on the size, may or may not be material. But companies need to understand the strategies used by regulatory agencies for enforcement. Most developed nations do not use monetary penalties as a form of revenue collection; rather, their intent is to change behaviour. If a company demonstrates cooperation and a true willingness to correct errant behaviour, monetary penalties are often mitigated and proportionate. However, egregious, fraudulent actions, or violations related to national security, can result in monetary fines in the millions of dollars – amounts large enough to send a clear message to others who might be so inclined. While financial penalties are effective in driving behaviour if they are large enough, the most concerning penalty for a high volume global trader is the possibility of debarment. The total loss of import or export privileges could in effect extinguish a company's existence in certain markets. Not good.

RC: What benefits can new technology and software offer as a mechanism for conducting due diligence and maintaining international trade compliance?

Neuschul: High quality global trade management software has been on the market for quite some time

now. There are tremendous benefits that a company can reap from automating its trade processes. This holds through from the basic, transactional level – such as housing trade data and interacting directly with brokers or forwarders – to very complex trade compliance programmes that manage sensitive technologies, deemed export considerations and multijurisdictional licensing requirements. These systems enable trade professionals to monitor compliance, speed up logistics processes, maintain integrity of the trade programme, and provide metrics and reporting capabilities. Trade automation is now a standard for a best-in-class trade compliance programme, and as companies have an ever-increasing trend of growing their global footprint, some level of trade automation is becoming essential.

Smith: New technology and software can provide control. The complexity of global regulations presents enough risk alone to keep a trader up at night, but the real challenge is volume. The sheer number of global transactions taking place during any given day, week or month can be overwhelming. Each transaction presents a risk on multiple fronts and systemic errors can impact hundreds of transactions if not identified quickly. Technology allows systemic controls to be embedded in the transaction at multiple levels that can notify someone when something goes wrong or, could completely stop a violative transaction. Further, advanced data analytics provides insight on risk management at a deeper level than ever before. Risks can be more easily identified, controls can be put into place, audits can be performed on 100 percent of the transactions and records can be produced to support due diligence using trade software.

Cruz: When business is conducted in countries that are subject to extensive sanctions, companies have to undertake appropriate due diligence measures, such as checks on ownership structures, to ensure that appropriate compliance measures are in force. Technology does enable easy access to data, with risk measurement and regulatory measures assisting implementation mechanisms.

Cone: Over the past decade, software has proliferated as a compliance and strategic trade tool. For example, multinationals utilise databases to identify trade opportunities such as countries producing low cost inputs, or the customs duties applicable in various countries where they intend to ship goods. While software is a helpful but non-authoritative guide for determining customs duties and relevant export controls, software is absolutely crucial to ensure compliance with respect to certain sanctions platforms, such as the US regime administered by the Office of Foreign Assets Control (OFAC). OFAC publishes a list of 'bad guy' companies, individuals and even cargo vessels that companies are forbidden to do business with. The list can

change without effective notice and violations can result in confiscatory government action. Under OFAC, companies need to know their customers, input details on new business partners and wait for the software to return a green light before entering into contracts.

RC: What final piece of advice can you give to companies in terms of developing and managing an effective international trade compliance programme, to reduce related risks?

Smith: Companies should develop and maintain a compliant culture. In the US, the Sarbanes-Oxley Act (SOX) did a great job of creating compliance awareness in the C-suite, so a good first step in developing an effective trade compliance programme is to align it with the finance/tax function organisationally which could also align it with SOX. The important of getting support from the CEO cannot be overstated. If need be, start with the CFO, but in either case, V-level support is paramount. And, it is usually pretty easy to get since they are the 'go to jail' people. They have a vested interest in making sure a compliance programme is successful. The next challenge will be getting the mid-management level to support the programme by making it part of their performance metrics. Remember, in a compliant culture, most people want to do the right thing; your job is to show them how.

Cruz: It is important for companies to monitor their trade-related performance in core areas such as export control, customs compliance and trade data management. Key performance indicators should also be created, with regular internal assessments, mitigation actions and implementation follow ups. Critical deviations from expected trends should also be identified and monitored. In addition, companies are well-advised to develop and implement a risk management process with a robust and 'waterproof' structure.

Cone: An effective programme begins with a top down commitment to compliance. Senior management should provide its full support to the global regulatory compliance effort and designate a manager responsible for it. A written compliance manual tailored to the company's operations should be implemented. The compliance manager should ensure that the compliance protocols set forth in the manual are followed, and perform periodic internal compliance audits. Internal controls should include protocols for addressing compliance failures, reporting violations to regulators where it is mandatory and disclosing them voluntarily when doing so is not required but is likely to produce governmental clemency. While a robust compliance programme requires time and money, the expenses and internal disruptions associated with enforcement actions can be far more costly. Nor should the lack of prior issues lull companies into complacency,

as agencies are full of surprises and always on the lookout for the next enforcement opportunity.

Neuschul: One of the primary considerations for developing a well functioning trade programme is to ensure that the company's management has an appropriate understanding of the importance of this function. Consequently, it is important to position the trade function at a high and central enough spot within the company management structure to enable it to have appropriate insight and ability to influence major business decisions – such as those pertaining to finance/tax and legal issues. The specifics of this will depend on the company's profile, global footprint and appetite for risk. It is also important that the global trade compliance leader has a profile that enables her or him to understand tax, legal, accounting, operations, logistics and other areas to provide full value to the company. A common mistake some companies have made historically is to base their trade compliance function solely within the logistics and transportation sector, which ultimately results in an inability to act proactively to manage compliance risks. R&C

EDITORIAL PARTNER

AlixPartners

www.alixpartners.com

AlixPartners is a leading global business advisory firm of results-oriented professionals who specialise in creating value and restoring performance. We thrive on our ability to make a difference in high-impact situations and to deliver sustainable, bottom-line results. The firm's expertise covers a wide range of businesses and industries whether they are healthy, challenged or distressed. Since 1981, we have taken a unique, small-team, action-oriented approach to helping corporate boards and management, law firms, investment banks and investors to respond to crucial business issues. For more information, visit www.alixpartners.com.

KEY CONTACT

Harvey Kelly
Managing Director and Global Leader,
Financial Advisory Services
New York, NY, US
T: +1 (646) 746 2422
E: hkelly@alixpartners.com

EDITORIAL PARTNER

Ambridge Partners LLC

www.ambridgepartners.com

Ambridge Partners LLC and its UK based subsidiary, Ambridge Europe Limited, is a specialised managing general underwriter of transactional, contingency and specialty management liability insurance products. Founded in 2000, the firm's mission is to provide its clients with customised solutions that facilitate the accomplishment of strategic objectives in connection with a wide variety of circumstances or situations such as financings & investments; licensing agreements; liquidations; mergers & acquisitions; and restructurings. Through working closely with its clients, Ambridge provides insurance solutions that are flexibly designed to meet individual requirements and delivered in an unobtrusive, timely and cost effective manner.

KEY CONTACTS

Tim Kennedy
Chief Underwriting Officer
New York, NY, US
T: 1 (212) 871 5403
E: tkennedy@ambridgepartners.com

Jefferey Doran
Managing Director
London, UK
T: +44 (0)20 3874 0052
E: jeffdoran@ambridgeeurope.com

Thomas Umstatter
Chief Operating Officer – International
New York, NY, US
T: 1 (212) 871 5420
E: tumstatter@ambridgepartners.com

EDITORIAL PARTNER

EY Advisory

www.ey.com

EY Advisory believes a better working world means helping clients solve big, complex industry issues and capitalise on opportunities to grow, optimise and protect their businesses. A global mindset, diversity and collaborative culture inspires EY consultants to ask better questions, create innovative answers and realise long-lasting results. The better the question. The better the answer. The better the world works.

KEY CONTACTS

Andy Reisman
Senior Manager
Boston, MA, US
T: +1 (617) 585 0302
E: andrew.reisman@ey.com

John Rogula
Senior Manager
Chicago, IL, US
T: +1 (312) 879 2379
E: john.rogula@ey.com

Dan Casciano
Principal
Greensboro, NC, US
T: +1 (336) 210 2740
E: daniel.casciano@ey.com

FISHERBROYLES
A LIMITED LIABILITY PARTNERSHIP

EDITORIAL PARTNER

FisherBroyles, LLP

www.fisherbroyles.com

FisherBroyles, LLP is a full-service law firm with 160 lawyers and 20 offices across the United States. Founded in 2002, FisherBroyles is the country's first and largest cloud-based law firm. Utilising the Law Firm 2.0® business model, FisherBroyles prioritises the highest quality legal services by partners who possess the most relevant expertise, while the firm's structure maximises efficiency, responsiveness and value. Focusing on long-term client satisfaction and not short term profits, FisherBroyles attorneys are full partners and veterans of some of the largest and most sophisticated law firms and corporate legal departments in the US. Rejecting the high fixed-cost structure of the traditional law firm model, the firm produces high quality work efficiently, and offers rates that are logical, predictable and flexible.

KEY CONTACT

Michael Cone
Partner
New York, NY, US
T: +1 (212) 655 5471
E: mcone@fisherbroyles.com

EDITORIAL PARTNER

IdentityMind

www.identitymind.com

Working with a broad spectrum of companies around the world, **IdentityMind's** mission is concise: construct electronic identities and infuse integrity back into the global market of digital commerce. We continue to enhance our core technology Electronic DNA (eDNA), capturing good and bad actors within the ecosystem in order to provide cost-effective risk management solutions while keeping the privacy of the actors. Together we are impacting and neutralising some of the most pressing issues facing our society and the financial ecosystem including money laundering, transactional fraud and boarding risk/Know Your Customer (KYC). Everyone at IdentityMind is deeply devoted to this mission.

KEY CONTACT

Garrett Gafke
President & Chief Executive Officer
Palo Alto, CA, US
T: +1 (650) 618 9977
E: garrett@identitymind.com

NAVEX GLOBAL®
The Ethics and Compliance Experts

EDITORIAL PARTNER

NAVEX Global

www.navexglobal.com

NAVEX Global helps more than 12,500 organisations worldwide contain compliance risks amid a never-ending stream of rapidly evolving internal and external threats. Our full suite of proven software, services and expertise helps ensure our clients' Ethics & Compliance programmes are proactive, thorough and effective. Our mission is to help organisations protect and defend their people, reputation and bottom line – and maintain a resilient, ethical organisational culture.

KEY CONTACTS

Ian Painter
Senior Marketing Manager, EMEA
Richmond, UK
T: +44 (0)208 939 1944
E: ipainter@navexglobal.com

EDITORIAL PARTNER

Paragon International Insurance Brokers Ltd

www.paragonbrokers.com

Paragon International Insurance Brokers Ltd is a leading financial and speciality lines broker, 100 percent owned by the management, operating in the Lloyd's of London and International Specialty markets. Our focus is on areas that present complex risk management and risk transfer challenges, because this is where we add the most value for our clients. The Mergers & Acquisitions/ Transaction Liability team consists of lawyers and insurance professionals with over 25 years of experience in the M&A insurance market. We have successfully arranged over 650 policies for transactions in most industry sectors and geographies.

KEY CONTACTS

Brian Hendry
Head of M&A
London, UK
E: bhendry@paragonbrokers.com
T: +44 (0)20 7280 8276

Tan Pawar
Senior Vice President
London, UK
E: tpawar@paragonbrokers.com
T: +44 (0)20 7280 8260

Sophie Wallace
Vice President
London, UK
E: swallace@paragonbrokers.com
T: +44 (0)20 7280 8234

RK&O | RICHARDS KIBBE & ORBE LLP

EDITORIAL PARTNER

www.rkollp.com

Richards Kibbe & Orbe LLP

Richards Kibbe & Orbe LLP is a dynamic and entrepreneurial law firm with deep experience and relationships in the financial markets and business community. With approximately 65 lawyers in New York, Washington, DC and London, the firm provides innovative legal solutions to a sophisticated range of clients across the investment and business spectrum, from hedge funds and investment banks to corporate boards and businesses enterprises. Founded in 1990, the hallmark of RK&O's lawyers is exceptional judgment, the ability to provide clients with creative solutions to the most difficult problems and a commitment to the highest calibre service in a cost-effective manner.

KEY CONTACT

James Walker
Partner
New York, NY, US
T: +1 (212) 530 1817
E: jwalker@rkollp.com

EDITORIAL PARTNER

Tokio Marine HCC

www.tmhcc.com

At **Tokio Marine HCC**, we focus on financial lines, including M&A insurance, operating out of offices in Barcelona, London and Munich; together forming the groups' centre of excellence for this line of business and jointly holding an extensive international client network. Tokio Marine HCC Group's major domestic and international insurance companies have a financial strength rating of AA- by S&P and Fitch Ratings, A1 by Moody's and A+ by A.M. Best. As such, we are considered to be a leading local provider with global reach and one of the most reliable and stable insurers in the market.

KEY CONTACTS

Deborah McBrearty
Head of Transaction Risk Insurance
Barcelona, Spain
T: +34 93 530 7393
E: dmcbrearty@tmhcc.com

Priscille Hérault
Transaction Risk Insurance Manager
Barcelona, Spain
T: +34 93 530 7386
E: pherault@tmhcc.com

Miguel Angel Hernandez
Transaction Risk Insurance Senior Underwriter
Barcelona, Spain
T: +34 93 530 7326
E: mahernandez@tmhcc.com

EDITORIAL PARTNER

Walkers

www.walkersglobal.com

Walkers is a leading international law firm. We provide legal, corporate and fiduciary services to global corporations, financial institutions, capital markets participants and investment fund managers. Our clients are the most innovative firms and institutions across the financial markets, and rely on us for our ability to provide solutions to their most important legal and business issues. Walkers is consistently ranked in the top tier of the leading global legal directories. Recognised for being a 'dynamic team that is very user friendly', a regular comment by clients is that Walkers is the "go-to" firm for offshore legal advice.

KEY CONTACT

Rolf Lindsay
Partner
Cayman Islands
T: +1 (345) 914 6307
E: rolf.lindsay@walkersglobal.com

ORGANISATION

Airmic

Airmic is the association for everyone who has a responsibility for risk management and insurance for their organisation. Members include company secretaries, finance directors, internal audit as well as risk and insurance managers. We support our members in a range of ways: through training and research by sharing information; through our diverse special programme of events; by encouraging best practice; and by lobbying on subjects that directly affect risk managers and insurance buyers. Above all, we provide a platform for professionals to stay in touch, to communicate with each other and share ideas and information.

John Hurrell
Chief Executive
London, United Kingdom
T: +44 (0)20 7680 3088
E: john.hurrell@airmic.co.uk

www.airmic.co.uk

ORGANISATION

Chartered Institute of Procurement & Supply (CIPS)

The **Chartered Institute of Procurement & Supply (CIPS)** exists to promote and develop high standards of professional skill, ability and integrity among all those engaged in purchasing and supply chain management. As an influential professional body, CIPS helps all kinds of organisations achieve all-round excellence in procurement and supply management. The organisation achieves this by offering a range of products and services to provide the knowledge, training and practical skills that are needed to derive maximum benefit from procurement practices. Established in 1932 and based in the UK, CIPS assists individuals, organisations and the profession as a whole.

David Noble
Group Chief Executive Officer
United Kingdom
E: press@cips.org

www.cips.org

ORGANISATION

International Center for Compassionate Organizations (ICCO)

The **International Center for Compassionate Organizations (ICCO)** works to foster cultures of compassion in government, business, healthcare systems, service agencies, colleges and universities, schools, faith groups and other organisations worldwide. The ICCO responds to the emerging trend among a broad range of organisations seeking to incorporate compassion as a value and practice in their relationships with their staff, colleagues, board members, customers and communities. The ICCO develops practical research, resources, education, consulting, coaching and conferences. It takes a nonpolitical, evidence-based and public health approach, and assists organisations to effectively improve employee engagement, productivity, staff retention, profitability and customer satisfaction.

Tony Belak
Associate Director General
Louisville, KY, US
T: +1 (502) 413 2123 ext. 2
E: tony.belak@compassionate.center

www.compassionate.center

THE INTERNATIONAL CENTER FOR
Compassionate Organizations

ORGANISATION

ICSA: The Governance Institute

ICSA: The Governance Institute is the professional body for governance. With over 125 years' experience working with regulators and policymakers, the organisation supports its members across all sectors of the economy, including large corporates, SMEs, the public sector, charities and academies. ICSA is the only organisation to confer chartered secretary status on those who are suitably qualified and experienced. Established in 1891, the knowledge and expertise of ICSA is rooted in history and continues to lead current thinking and practice. ICSA's stated guiding values are openness, integrity and authority.

Simon Osborne
Chief Executive Officer
London, UK
T: +44 (0)20 7612 7001
E: ceo@icsa.org.uk

www.icsa.org.uk

icsa

ORGANISATION

ISACA

ISACA helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus (CSX), a holistic cyber security resource, and COBIT, a business framework to govern enterprise technology.

Eva Sweet
Technical Research Manager
Chicago, IL, US
T: +1 (847) 660 5581
E: esweet@isaca.org

www.isaca.org

ISACA®
Trust in, and value from, information systems

ORGANISATION

The WomenCorporateDirectors Education and Development Foundation, Inc.

The WomenCorporateDirectors Education and Development Foundation, Inc. (WCD Foundation) is the only global membership organisation and community of women corporate directors. A 501(c)(3) not-for-profit organisation, the WCD Foundation has 74 chapters around the world, with seven more to launch over the next year. The aggregate market capitalisation of public companies whose boards WCD Foundation members serve on is over $8 trillion. In addition, WCD Foundation members serve on numerous boards of large private and family-run companies globally.

Susan Stautberg
CEO, Co-Founder and Co-Chair
Palm Beach, FL, US
T: +1 (561) 290 0389
E: sstautberg@womencorporatedirectors.com

www.womencorporatedirectors.com

wcd WomenCorporateDirectors FOUNDATION
globally accelerating best practices in corporate governance

OCT-DEC 2016
www.riskandcompliancemagazine.com