Inside this issue:

FEATURE
Determining risk appetite

EXPERT FORUM
Managing risk when hiring new employees

HOT TOPIC
Planning for shareholder activism
ANY TIME.
ANYWHERE.
ANY MATTER
OF RISK.

Global Corporate Compliance
CONTENTS

004 FOREWORD
007 FEATURE
  Determining risk appetite
013 FEATURE
  Promoting diversity in the boardroom
186 EDITORIAL PARTNERS

019 EXPERT FORUM
  Managing risk when hiring new employees
  1stWEST Financial Corporation; Goodwin Procter LLP;
  Littler Mendelson; Norton Rose Fulbright; Skadden, Arps,
  Slate, Meagher & Flom LLP
038 PERSPECTIVES
  Communicating the cyber crime threat to the
  UK’s c-suite
  Advent IM Ltd
042 MINI-ROUNDTABLE
  Managing risk and security issues arising from mobile access
  Hogan Lovells US LLP; Pillsbury Winthrop Shaw Pittman;
  Poyner Spruill LLP; Symantec
057 PERSPECTIVES
  Nailing data breach notification – best practices for consumer confidence
  Experian Data Breach Resolution
060 MINI-ROUNDTABLE
  Anti-corruption and compliance in the energy sector
  EY
068 PERSPECTIVES
  Don’t be an ostrich: liability under the FCPA for ignoring indications of possible bribery
  Baker & McKenzie LLP
075 MINI-ROUNDTABLE
  Impact of Brazil’s Clean Companies Act
  Berkeley Research Group; Koury Lopes Advogados; Mattos
  Muriel Kestener Advogados; Trench Rossi & Watanabe

www.riskandcompliancemagazine.com
<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>091</td>
<td>ONE-ON-ONE-INTERVIEW</td>
<td>Fraud investigations by multilateral development banks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bretton Woods Law</td>
</tr>
<tr>
<td>096</td>
<td>PERSPECTIVES</td>
<td>Mitigating the risk of mounting conflict mineral sourcing regulations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3E Company</td>
</tr>
<tr>
<td>100</td>
<td>MINI-ROUNDTABLE</td>
<td>International cartel enforcement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gibson, Dunn &amp; Crutcher LLP; Hogan Lovells International LLP; Norton Rose Fulbright South Africa; Shearman &amp; Sterling LLP</td>
</tr>
<tr>
<td>116</td>
<td>PERSPECTIVES</td>
<td>Risks in selecting the wrong governing law and forum</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gould &amp; Ratner LLP</td>
</tr>
<tr>
<td>120</td>
<td>MINI-ROUNDTABLE</td>
<td>Advice for non-EU fund managers on AIFMD compliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Davis Polk &amp; Wardwell London LLP; King &amp; Wood Mallesons LLP; Schulte Roth &amp; Zabel International LLP</td>
</tr>
<tr>
<td>130</td>
<td>PERSPECTIVES</td>
<td>The biggest risk of all: success</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Solon Group, Inc.</td>
</tr>
<tr>
<td>134</td>
<td>PERSPECTIVES</td>
<td>Cultivating a winning culture</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Black Diamond Associates</td>
</tr>
<tr>
<td>138</td>
<td>PERSPECTIVES</td>
<td>Understanding and managing strategic risk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Neill Buck &amp; Associates</td>
</tr>
<tr>
<td>143</td>
<td>PERSPECTIVES</td>
<td>The role of organisational change in effective enterprise risk management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cambio Consulting Group</td>
</tr>
<tr>
<td>148</td>
<td>PERSPECTIVES</td>
<td>Risk management oversight: a debate continues and audit committees get busier</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Willkie Farr &amp; Gallagher LLP</td>
</tr>
<tr>
<td>151</td>
<td>PERSPECTIVES</td>
<td>Giving voice to values in the boardroom: strategies to enable risky conversations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GEC Risk Advisory LLC and Giving Voice To Values</td>
</tr>
<tr>
<td>155</td>
<td>PERSPECTIVES</td>
<td>The lack of strategic information can leave money on the table</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FiscalDoctor</td>
</tr>
<tr>
<td>158</td>
<td>PERSPECTIVES</td>
<td>Mitigating reputation risk for success: strategic planning in today’s multi-stakeholder, multi-channel environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reputation Institute</td>
</tr>
<tr>
<td>162</td>
<td>PERSPECTIVES</td>
<td>Weathering the storm: companies will need to take steps to assess and manage climate risks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Center for Climate and Energy Solutions</td>
</tr>
<tr>
<td>167</td>
<td>HOT TOPIC</td>
<td>Planning for shareholder activism</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Innisfree M&amp;A Incorporated; McDermott Will &amp; Emery LLP; RLM Finsbury; Skadden, Arps, Slate, Meagher &amp; Flom LLP</td>
</tr>
</tbody>
</table>
Has your company competed for or won contracts financed by the Multilateral Development Banks? If the answer is ‘yes’ then you should ask yourself whether you or your company are at risk of committing, or have committed, a sanctionable practice?

Companies which fall foul of the Multilateral Development Banks’ (the ‘MDBs’) anti-fraud and corruption requirements, even through ignorance, can face sanctions, including possible debarment or worse. When this happens, you need to act quickly to find effective solutions. Bretton Woods Law has world-class credentials in this field and can provide and implement a strategy to best defend the company’s interests.

To help you to avoid the risks of debarment and automatic cross-debarment, Bretton Woods Law invites you to join others from the MDB community at the inaugural Multilateral Development Bank Anti-Corruption Sanctions Conference.

Multilateral Development Bank
Anti-Corruption Sanctions Conference
London, 20th - 21st November 2014

TO REGISTER YOUR INTEREST, CLICK HERE
Welcome to the seventh 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 risk appetite and diversity in the boardroom. We also look at: risks when hiring new employees; cyber crime; security issues arising from mobile access; data breach notification; anti-corruption in the energy sector; liability under the FCPA; Brazil’s Clean Companies Act; fraud investigations by multilateral development banks; international cartel enforcement; advice for non-EU fund managers on AIFMD compliance; understanding strategic risk; giving voice to values in the boardroom; managing climate risks; planning for shareholder activism; and more.

Thanks go to our esteemed editorial partners for their valued contribution: 1stWEST Financial Corporation; Baker & McKenzie; Berkeley Research Group, LLC; Bretton Woods Law; EY; Goodwin Procter; Innisfree M&A Incorporated; Poyner Spruill; RLM Finsbury; Shearman & Sterling; Cambio Consulting Group; Giving Voice to Values; C2ES; and the Reputation Institute.

– Editor
Risk is a great motivator. But let it distract you, and you risk everything.

It’s getting tougher out there. Risks of fraud, bribery and corruption are up, and pressure on regulatory compliance is rising. But we can help you handle sensitive situations and find ways to reduce risk – so you can get back to business.

Learn how at ey.com/uk/fids.

Contact David Lister, Oil & Gas Sector Lead – Fraud Investigation and Dispute Services on Office: +44 (0)131 777 2308 or dlister@uk.ey.com
Risk oversight and governance is one of the most crucial areas for boards of directors and C-suite executives. Should companies fail to acknowledge risk, and their relationship with that risk, they could ultimately expose the firm to greater damage when something goes wrong. Equally, if companies fail to take on enough appropriate risk, they make it much more difficult to achieve their goals and the growth required in today’s business climate.

The issue of risk management has become much more pertinent since the onset of the financial crisis. The crisis, along with the high profile bankruptcies and defaults it brought, helped to bring risk and risk management sharply into focus. Arguably, in the period immediately preceding the global financial crisis, warnings were overlooked. Risks were missed, understated or simply ignored. Banks, regulators, supervisors, investors and others were all guilty of taking a flawed approach to risk and risk management policies.

Although the financial crisis had an extremely detrimental effect on the global economy, it did have some positive side effects. Thankfully, as a result of the crisis, attitudes towards risk have begun to shift across a wide variety of sectors, and firms are becoming much more willing to embrace risk management strategies. This shift is largely a result of increased regulatory pressures. Acts such as Dodd-Frank have placed a greater focus on
corporate governance and proven a catalyst for change.

To that end, companies now accept that at the heart of their approach to risk management should be a clearly defined and managed level of risk appetite. Although risk appetite has been a notoriously difficult concept to define, when it is properly understood it can be a potent tool in any firm’s enterprise risk management (ERM) program. However, risk appetite and the parameters of a firm’s appetite can be complicated. In its simplest terms, risk appetite determines how much risk an organisation is willing to assume consistently within the confines of its wider ERM strategy. Given that almost every business strategy adopted will involve some degree of risk, it is imperative that companies clearly define their risk appetite. Risk appetite forms an essential element of ERM, in so much as it allows firms to clearly define their current risk profile.

Internal debates around the appropriateness of a company’s risk appetite can be confusing, and incorrect terminology is often employed. Such errors can lead to further uncertainty. When executives do not have a clear understanding of their company’s risk appetite on an operational level, the firm may find that certain middle management decisions, for example, go against the assumed risk appetite set out by executives or board members. In the modern climate, an informal or inappropriate approach to risk capacity and appropriateness can prove disastrous for companies. Furthermore, an unsuitable approach to risk appetite can cause a company’s EMR program to stagnate rather than evolve and adapt in line with any strategic and business changes that occur.

ERM schemes provide firms with a wider framework for risk management, while also helping companies to identify relevant risks and opportunities. Businesses can utilise ERM to assess those risks and opportunities in order to determine the likelihood and extent of their impact on the firm. Furthermore, ERM allows companies to develop a response strategy to any issue which might arise. By identifying and proactively addressing risks and opportunities, ERM programs can not only protect the overall business, they can also help to create value for the firm’s stakeholders, including the company’s ownership, employees, customers, regulators, and society overall.

Role of the stakeholder

Establishing an appropriate risk appetite can be a complicated task, but there are a number of significant advantages for firms which take the time to articulate their approach to their stakeholders. Arriving at a clear and well defined definition of risk appetite will help the company to achieve a number of important goals. It will plainly establish the types of risk the firm wants to take on, and the amount of risk the firm considers acceptable. The firm will also make clear, to all stakeholders, the attitudes of the company’s board and C-level executives towards risk.
A subject as important as risk appetite should clearly form an integral part of any company’s broader business strategy, residing, as it does, at the centre of how firms conduct their day to day business. As such, the main thrust of a company’s approach to risk appetite should be provided by its board and C-level executives, who can provide a top down approach to the concept of risk. However, the responsibility for establishing a company’s risk appetite does not sit entirely on the shoulders of the board; board members should converse with, and take into account the expectations and beliefs of the firm’s shareholders, regulators and other stakeholders when determining risk appetite.

Furthermore, boards should take into account the wider risk landscape of their sector when formulating their own risk appetite. Factoring both internal and external reactions to recent risk events will help to determine the company’s true risk appetite.

The CRO

Much of the work in establishing a company’s risk appetite should be coordinated by the chief risk
officer (CRO). The CRO is a relatively new position in the boardroom, yet the role has risen to a level of great prominence in the last few years. In the modern boardroom, CROs should take responsibility for directing the dialogue around the definition and revision of the firm’s risk appetite.

In adopting a top down approach to matters of risk, board members, including non-executive directors, need to engage with the subject. This level of communication will provide a healthy and informed framework that can be utilised by the firm to articulate its approach to, and appetite for, risk. Companies can also ensure that their senior executives present a united front on the subject of risk appetite. It is easier to circulate a message on this potentially volatile topic if the company’s leaders are all singing from the same hymn sheet.

However, once the firm’s board – with input from other stakeholders and interested parties – has determined the company’s wider risk appetite, it is crucial that the process isn’t neglected. Outlining a company’s risk appetite strategy should not be viewed as a onetime occurrence. Risk appetite should be placed under constant review as part of the company’s ERM program. Treating risk management as an ongoing process will benefit the whole company. Although firms in some sectors, such as banking and financial services, are required by regulators to have a risk appetite statement in place, risk appetite is much more than a mere statement – it promotes a particular culture.

Defining a clear and comprehensive risk appetite establishes a baseline for further risk based dialogue.

“Defining the firm’s risk appetite should begin with a full understanding of its wider strategic goals and objectives, stakeholder perspectives, risk culture and risk experience.”

Companies can expand upon this baseline and shape their long term risk appetite in line with the firm’s culture of risk – the direction and flow of capital allocation and investments, in particular, should be shaped by the firm’s risk appetite. In turn, risk appetite should be influenced by external forces. Changes in the business environment, economic conditions, competition and other factors should all feed into the development of a robust, adaptable and well defined risk appetite.

Employees should play a part in the company’s ERM strategy. Training programs, as part of a top down approach determined by the company’s
board, should be arranged for employees. Such training schemes will help employees understand the company’s risk appetite and the impact it will have on their everyday activities. Furthermore, regular training events can encourage employees to adopt desired behaviours and cultures. Firms may also find it advantageous to embed risk appetite into business activity planning, as well as relevant company policies and procedures as part of their ERM strategy.

When determining an appetite for risk, there are many factors that companies should take into account. One of the more important of these is the firm’s attitude towards risk in the context of its overall desire for growth and returns. However, different interest groups often have disparate expectations of returns, which can lead to discord. Often companies focus primarily on the appetite of one particular group without paying sufficient heed to the appetites of others. As we have seen from 2008 onwards, failures relating to risk can be disastrous for companies, and even entire sectors. Many companies that miscalculated the relationship between risk and return since the onset of the financial crisis have gone out of business; those that experienced financial difficulty but survived the downturn still suffered reputational risk as a result.

Defining the firm’s risk appetite should begin with a full understanding of its wider strategic goals and objectives, stakeholder perspectives, risk culture and risk experience. Based on this foundation, the firm’s management should continue to develop the risk appetite process, taking into account the company’s risk profile and risk capacity. Qualitative risk assessments, and quantitative risk analysis and limits, should also be factored in. A qualitative risk assessment will see the firm’s leaders categorise and prioritise top individual risks, relative to one another, based on risk, reward and risk mitigation activities.

A quantitative risk analysis will see firms use a rating scale in order to provide a greater degree of precision and measurability to its various risks. Rating scales can take many forms, such as estimates, benchmarking and more complicated probability models. Both models help to contribute to the firm’s development of a realistic and well defined risk appetite. By utilising tools such as these, firms can determine exactly how much risk is acceptable in order to pursue and achieve their wider growth objectives.

Today, more than ever, risk appetite should play a fundamental role in the development of a company’s wider business strategy. If business leaders are able to learn from the mistakes of the period immediately preceding the financial crisis, and can clearly define their firm’s approach to risk, they can unlock significant value. Accordingly, sensible decision making around risk is the key to future success. RC
Risk & Compliance is an e-magazine dedicated to the latest developments in corporate risk management and regulatory compliance.

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
Companies operating in today’s business climate face a number of significant concerns and challenges. One of the most important considerations revolves around the concept of diversity, in the boardroom and at the non-executive level.

Most companies want to achieve diversity but often do not know how to realise their goal. Diversity can be a difficult concept to grasp. Often the emphasis lies with companies recruiting non-white executives and directors and expecting those new hires to blend in sufficiently with the company’s existing corporate structure. There are some who see the clamour for greater diversity in the boardroom as little more than an exercise in political correctness. However, a topic as important, and as challenging, as diversity should not be so easily dismissed.

It stands to reason that the backgrounds of board members should reflect the nature of the business they represent. Over the last 20 to 30 years, not only have we seen firms becoming more complex, we have also seen a huge swing towards globalisation and heightened regulation. The business world, like society in general, has changed, and a more diverse group of business leaders may be required to take businesses forward.

Diversity issues tend to be more pronounced when they involve a firm’s upper echelons. Assembling a high quality board of directors can be
a difficult task. Each member of a company’s board must bring her own abilities and dynamism to the role. Equally, candidates to the board must be of sufficient calibre to elevate the group. Furthermore, the right boardroom candidates must also bring her own individual perspectives and personality traits to the position, but not in a way that hinders the effective execution of corporate governance and strategic oversight. Individuals nominated to the board must be experienced, responsible and open to collaboration with their colleagues. They must be able to identify and evaluate risks and opportunities wherever possible, and provide the firm’s chief executive with considered, sensible counsel.

Often, it is the question of experience which bars underrepresented groups from appointment to boards and senior positions. Firms want their boards to be occupied by experienced and knowledgeable members. This leads to a catch-22 situation: how can you gain experience if you are not given the opportunity to do so?

One argument suggests that the reliance of firms on experienced candidates – generally white males – has been exacerbated by the rigours of the global financial crisis. “With companies focused on survival, their boards stuck with the team of directors they had rather than change mid-crisis,” says Victor Arias, Jr, a senior client partner at Korn Ferry. “When new members were recruited they were most often former CEOs and CFOs with experience navigating challenging times.”

Attitudes to boardroom diversity are beginning to change, albeit slowly. Such developments can be seen from an operational standpoint. In recent years, new positions such as chief risk officer and chief technology officer have come to the fore, giving new prominence to roles previously considered to be fairly minor positions. The promulgation of such positions at the executive level is an indication that companies are beginning to adapt to change, and engaging with new ideas.

But, despite these encouraging developments, the composition of boards has not changed anywhere near as notably. They remain largely homogenous. The boardroom is still regarded as the domain of white males. “Corporate boards remain remarkably unreflective of both the workforce and markets served,” says Brande Stellings, vice president of Corporate Board Services at Catalyst, a non-profit organisation which expands opportunities for women and business. “Eighty-three percent of Fortune 500 directors are men and 84 percent of board seats are occupied by whites or Caucasians. These findings are generally consistent across the globe. Yet a whole body of research indicates that diversity benefits decision-making, innovation and the bottom line”.

Support for boardroom diversity does appear to be growing. Some argue that greater diversity in the boardroom, especially with regard to women, could have gone some way to avoiding or at least mitigating the effects of the global financial crisis. In
the UK, Women in the City, a report from the Treasury Select Committee, highlighted the need for reform, particularly in the financial sector. According to the committee’s findings, a lack of female representation in the boardroom has led to the promotion of a dangerous culture of homogeneity among male board members. The group mentality of men in the boardroom has made the scrutiny of executive decisions markedly less effective. Research shows people from the same background with similar experiences are less likely to challenge one another on their actions.

Calls for firms to embrace diversity are growing louder, not only as a pragmatic response to the changing world we live in, but also as a considered and responsible business decision. Diversity in the workplace can have a number of positive benefits for boards and companies in general. Nevertheless, the pace of change is nowhere near quick enough. But how can companies promote and embrace diversity at the highest level?

Some analysts have suggested quotas would be an effective means of diversifying the boardroom, and a number of regulators and politicians have considered this. Notably, in 2003, the Norwegian government introduced quotas dictating that women should occupy 40 percent of a board’s seats. However, there is considerable opposition to such quotas. Critics fear that this system can lead to trophy or token appointments, something which has been seen in Norway. While recognising the drawbacks, Mr Arias is in favour of building the case for quotas. “While quotas are not the preferred route to achieving diversity, sometimes they have to be mandated if progress is ever to be achieved. Quotas were popular in the US in the 60s and 70s with affirmative action programs. The change was very noticeable in corporate America and higher education.”

Yet, as Ms Stellings notes, efforts must go further. “Quotas are one proven strategy but measures to increase women’s representation on corporate boards need to be culturally appropriate and relevant, keeping in mind what will achieve the right outcome. We see that a variety of approaches have accelerated momentum, including voluntary efforts...”

“Calls for firms to embrace diversity are growing louder, not only as a pragmatic response to the changing world we live in, but also as a considered and responsible business decision.”
as well as mandating a ‘comply or explain’ reporting scheme,” she says.

While, in the short term, quotas may elevate women to board positions through token appointments, the long term outcome of greater boardroom diversity must surely be seen as a positive step. The emphasis for companies should shift towards ensuring that an adequate pipeline is in place for female talent to rise to board level. Increased emphasis should be placed on firms’ recruitment and succession planning methods to ensure the right people progress, regardless of their sex or ethnic background. And this should not be limited to the boardroom.

The advantages to promoting diversity are myriad. It opens up discourse, enabling firms to engage with a wide range of perspectives. Multiple viewpoints provide greater insight into the various risks, consequences and implications of a company’s actions. Since the onset of the financial crisis, many firms have found themselves facing increasing levels of scrutiny from investors, the media, regulators and other non-governmental organisations. In light of this increased exposure, companies are seeking directors that have experience dealing with risk from many angles. Having directors and executives from a wide spectrum of backgrounds could certainly help in that regard.

Institutional investors have been a key driver of the diversification process. “They have been able to exert a great deal of influence and have been a
potent, positive force for change in the boardroom, including demands for greater diversity,” says Mr Arias. “There is growing evidence to support the argument that greater diversity on boards translates into greater returns to shareholders. Consequently, institutional investors have filed shareholder resolutions urging companies that are lacking in diversity on their boards to commit to achieving greater diversity. They are also pushing for greater transparency in the selection process for new directors”.

Increasingly, institutional investors are making their voices heard. Since the so-called investor spring of 2012 there has been a notable increase in investor influence in boardrooms, with activist investors having their say on many corporate governance issues. With regards to diversity, investors are utilising both private persuasion and public pressure to influence board appointments. Ultimately, money talks and there is research suggesting that companies with more women on their boards perform well financially and are better governed. Taking improved financial performance into account, if investors want to see greater diversity in the boardroom, it is likely to happen. By making increasingly public calls, investors and regulators are making it difficult for companies that drastically under-represent women and minorities to hide.

In recent years, slow but steady progress has been made in the field of boardroom diversity, and not before time. However, the process is by no means
complete. There is still a long way to go before the boardroom becomes a level playing field. So how will boardroom diversity develop from here?

The key developments will be long-term rather than immediate. Much of the progress will require cultural shifts and these types of developments take time to ingrain themselves in corporate cultures. “This require a broad understanding of why diversity is important from a business standpoint, including respecting our individual differences, understanding the perspectives of key constituencies, and the value of promoting an inclusive environment in the boardroom and throughout the enterprise,” says Mr Arias. “This change will happen by design, not by accident, and implementing financial incentives for CEOs and other senior managers to promote greater diversity should be part of the solution.”

The fight for boardroom diversity will be a long one, but will ultimately be successful, according to Ms Stellings. “Get ready for change, albeit slowly and steadily. The drumbeat for increased diversity in the boardroom is getting louder. Government and private-public initiatives have been gaining traction. For the first time in years, the 2013 Catalyst Census: Financial Post 500 Women Board Directors has reported an uptick in the representation of women on public boards. With global conversation and activity accelerating, companies need to lead or get left behind,” she says.

As regulatory and shareholder pressure on companies intensifies, boards must resolve to push through changes wherever applicable, creating systems and cultures which position individuals to maximise their potential regardless of gender, cultural background, age, education, class or ethnicity. By diversifying in this way, companies will be able to placate stakeholders while generating growth and driving returns.  

RC
EXPERT FORUM

MANAGING RISK WHEN HIRING NEW EMPLOYEES
**PANEL EXPERTS**

**Jerry Oldham**
Chairman and CEO
1stWEST Financial Corporation
T: +1 (303) 670 3443
E: j.oldham@1stwest.com

Jerry Oldham has an extensive investigations and corporate due diligence background, and a broad senior management resume in commercial banking and corporate and real estate finance. He frequently serves as a consultant or expert witness in litigation and settlement negotiations involving complex corporate finance, real estate, banking, and lending practice issues, having assisted in the settlement of hundreds of lawsuits.

**Robert M. Hale**
Partner
Goodwin Procter LLP
T: +1 (617) 570 1252
E: rhale@goodwinprocter.com

Robert M. Hale, a partner in and chair of the Goodwin Procter LLP’s Labor & Employment Practice, represents employers across a broad spectrum of employment matters. Mr. Hale’s practice involves representation of clients in employment litigation, including noncompetition, discrimination, wrongful discharge, FLSA and ERISA litigation. He has obtained successful results for employers at all stages of litigation, including in preliminary injunction proceedings, at summary judgment, at trial and on appeal. Mr. Hale is experienced in successfully representing employers before administrative agencies and in labour arbitrations. His practice also includes counselling in numerous areas of labour and employment law.

**Philip Berkowitz**
Partner
Littler Mendelson
T: +1 (212) 497 8481
E: pberkowitz@littler.com

Philip Berkowitz, US co-chair of Littler Mendelson’s International Employment Law Practice, advises multinational and domestic companies in lawsuits and arbitrations, in the United States and internationally, in discrimination and harassment, compensation, whistleblowing and other anti-retaliation, trade secret and non-compete claims. Mr Berkowitz’s clients include financial services, oil and gas, pharmaceuticals and chemicals, manufacturing, publishing, fundraising, and other industries. He has also represented prominent international law firms in their employment law matters.

**T. Jeff Wray**
Partner
Norton Rose Fulbright
T: +1 (713) 651 5585
E: jeff.wray@nortonrosefulbright.com

Jeff Wray is the partner in charge of the Houston office labour and employment practice of Norton Rose Fullbright. Since 1974, he has represented employers in labour and employment matters in federal and state trial and appellate courts and before administrative agencies such as the National Labor Relations Board (NLRB), the Department of Labor and the Equal Employment Opportunity Commission (EEOC). His practice includes: jury and bench trials of employment cases; counselling concerning international law, including trans actions and employment agreements; representing management in union organisational campaigns and preventive efforts; and conducting collective bargaining agreement negotiations on behalf of employers.

**Risa Salins**
Counsel
Skadden, Arps, Slate, Meagher & Flom LLP
T: 1 (212) 735 3646
E: risa.salins@skadden.com

Risa Salins is a counsel in the Labor and Employment Law Group of Skadden, Arps, Slate, Meagher & Flom LLP. Ms Salins regularly advises companies on labour and employment matters arising out of complex US and multinational corporate transactions. She also counsels employers on a wide range of workplace issues, including compliance with antidiscrimination laws, employee privacy issues, plant closings and layoffs, accommodations for disabled workers, whistleblower protections, wage and hour laws, workplace safety and health and issues arising under the National Labor Relations Act. In addition to her practice, Ms Salins is a co-author of the labour law column for the New York Law Journal.
RC: Could you briefly discuss some of the key challenges and risks associated with hiring new employees? What mistakes do firms commonly make during the process?

Oldham: The primary challenges and risks are not verifying backgrounds, credentials, experience and education. Essentially, you don’t know what you don’t know. So, performing a background investigation is necessary.

Hale: There are at least three areas where we repeatedly see problems arise. First, an employer should know those it hires. An employee with performance problems is often the result of a hiring process that was incomplete, insufficiently rigorous or both. An employer has a number of tools at its disposal. It can direct its interviewers to focus clearly on how well an applicant’s established skill set meets its needs. It can conduct reference checks that also focus on the skill sets applicable to the position. It can use social media, as long as it does so without pretexting or misusing information from social media sources. It can get further background information through a background check. There is considerable scepticism about the utility of each of these tools in isolation, but by using all of them in a focused and rigorous manner, an employer can be in a better position to identify the best candidates. Second, employers should make sure that interviewers know some basic employment discrimination rules that apply to hiring. Legal claims arising from hiring decisions most often are based on statements made in interviews. The most challenging aspect of the law that affects interviewing concerns disability-related questions. With very limited exceptions, interviewers should not ask about medical problems or workers’ compensation absences. An employer may obtain a medical examination after making a job offer that is conditioned on the examination, but it generally needs to avoid making pre-offer inquiries relating to possible disabilities. In addition, although employers have become more sensitised over the years to avoiding inquiries about pregnancy and other family considerations, we still learn of missteps by employers in asking questions that can tend to screen out candidates on the basis of pregnancy specifically or gender in general. Moreover, with an increase in the number of older applicants seeking jobs, employers need to avoid stereotypical assumptions about energy level and the anticipated commitment to jobs, and interviewers certainly need to avoid asking questions that suggest that they are making such assumptions. Third, employers too often do not learn of or sufficiently explore possible non-competition and non-solicitation issues during the hiring process. Some employers believe that obligations under non-competition and non-solicitation agreements can be easily avoided.
Sometimes those agreements are overreaching and unenforceable, but often they are enforceable. Employers should be careful before making commitments to new hires to indemnify them against liability and attorneys’ fees in connection with non-competition and non-solicitation agreements.

**Berkowitz:** Perhaps the biggest mistake that companies make in hiring new employees is misclassifying them either as independent contractors or consultants, or as exempt from the federal and state laws mandating payment of overtime. Employers may seek to avoid providing benefits to new hires and therefore either accept an invitation to retain them as consultants, or impose this status on them. This is a very risky practice because it can lead to significant liability for unpaid overtime and back taxes. Also, improperly classifying individuals as ‘exempt’ from overtime laws can lead to the same liability. The law in the United States prohibits discrimination based on many factors, including age, gender, religion, race, colour, pregnancy and disability. It is almost always illegal to base a hiring or firing decision based on an individual’s age, no matter how old the individual may be. This is often a difficult reality for foreign companies doing business in the United States to understand. Mandatory retirement on the basis of age is almost always illegal. The misuse of social media in checking candidates’ backgrounds also presents great risk of claims of unlawful discrimination.

**Wray:** Employers in the United States sometimes complain that they are pulled in opposite directions with respect to the legalities of the hiring process. They face a claim of ‘negligent hiring’ if they fail to properly vet an applicant who is hired and subsequently causes harm to other employees or members of the public, and it is shown that a prudent employer would have discovered something in the applicant’s background which would have kept the employer from hiring the applicant. On the other hand, state, federal and local governments have enacted laws that limit both the process employers
can use to gather information and the use to which information which is gathered may be utilised in the hiring process. For example, under the Americans with Disabilities Act (ADA), employers may not request medical information from an applicant until they have first made an offer of employment conditioned only on the outcome of a medical evaluation. If the applicant is then rejected for any medically related reason, including alcoholism or a history of illegal drug use, the employer must be in a position to show that the medical condition would have kept the applicant from properly performing the job applied for, even with reasonable accommodation provided by the employer.

**Salins:** It is a challenge to properly vet applicants while at the same time assuring your company does not run afoul of anti-discrimination laws. Certain pre-employment inquiries have insufficient job relatedness to outweigh their potential adverse effect on job prospects of individuals protected from discrimination. To avoid potential discrimination claims, firms should train employees not to ask applicants questions that relate to a protected status, such as questions about race, religious affiliation, national origin, citizenship, sexual orientation, marital status or family responsibilities, age, disabilities, pregnancy, genetic information or military service. Today employers are increasingly using social media to recruit and scrutinise employee candidates, but these sites could expose employers to more information than they are legally allowed to ask during interviews. A common mistake is failing to have appropriate procedures in place to ensure social media searches are performed, or not performed, consistently on all candidates and that protected class information is not disclosed to hiring decision-makers.

**RC:** What regulatory changes have you seen in the US over the past 12-18 months? What has been the impact of the Fair Credit Reporting Act (FCRA)?

**Hale:** For the most part, significant regulatory developments affecting hiring come from the Equal Employment Opportunity Commission (EEOC). In 2012, a bit more than 18 months ago, the EEOC issued guidance on the use of arrest and conviction records in hiring. That guidance observed that using criminal records in hiring can have a disparate impact on minority group applicants. The guidance basically took the position that the fact of an arrest should not be a basis for rejecting an applicant, although conduct that led to an arrest could be a legitimate consideration, if the information is sufficiently reliable based on something other than the fact of the arrest. By contrast, the EEOC acknowledged that a conviction could be sufficient basis to show that an individual engaged in criminal conduct. At the same time, it said that a conviction should not be an absolute bar to employment. The
EEOC said that an employer should apply the three factors that were established in the case of Green v. Missouri Pacific Railroad in considering a conviction record. The ‘Green factors’ are the nature and gravity of the offense or conduct, the time that has passed since the offence or conduct or completion of the sentence, and the nature of the job sought. The Green factors were well accepted in the employer community as factors to consider before the EEOC guidance was issued. What is controversial about the EEOC position is that the EEOC said that the Green factors were only a ‘starting point’ and that an employer may in some cases need to go beyond the Green factors and apply several other factors in making an ‘individualised assessment’ concerning the relevance of a conviction to a hiring decision.

Salins: We have seen significant evolution in the regulatory environment of employment background screening in recent years. In April 2012, the EEOC issued enforcement guidance regarding use of arrest and conviction records in employment decisions, responding to what it considers a practice that disproportionately affects racial and ethnic minorities. Among other things, the guidance emphasises the need for criminal history information to be “job-related and consistent with business necessity”, and encourages employers to make an “individualized assessment” before using criminal history in an employment decision. In an effort to enforce its guidance, the EEOC over the last year brought disparate impact discrimination suits against numerous employers that have blanket criminal background check policies. We have also seen an increase in class-action lawsuits against employers regarding violations of the FCRA, the federal law that protects the privacy and accuracy of background information obtained by third party consumer reporting agencies. The claims include that employers failed to obtain from applicants or employees adequate authorisation to conduct background checks or failed to provide copies of background reports to applicants or employees before taking adverse employment actions. Recent settlements in these FCRA lawsuits have ranged between $2.5m and $3m.

Wray: Among the most significant regulatory developments in the past year is the publication in March 2014 by the Office of Federal Contract Compliance Programs (OFCCP) of rules requiring for the first time that federal contractors required to use affirmative action plans set a specific goal that 7 percent of each job group in their workforce be comprised of qualified individuals with disabilities. Additionally, a ‘benchmark’, which OFCCP says is not a ‘goal’ such as those applicable to women and minorities, must be adopted for military veterans. While special circumstances may warrant a higher or lower target, OFCCP has set a national benchmark of 8 percent which employers may adopt instead of analysing other availability data. The new rules
require employers to modify their affirmative action plans for plan years which begin after the rules went into effect. Employers are troubled by the requirement that they invite applicants to self-identify themselves as disabled at the pre-offer stage, fearing that this may lead to more claims by rejected applicants of discrimination even though the information will be kept as a record separate from the application. The FCRA has been in effect since 1968, but some smaller employers in particular are unaware of its requirements, and some small companies which specialise in background checks are also clueless. Where an employer conducts background checks itself, there are no FCRA implications. The FCRA only applies if an employer hires a third party to perform a background check on an applicant. In that instance the employer must obtain the applicant’s written consent to conduct the check. Before the applicant is rejected based on information turned up by the agency, the employer must provide the applicant a copy of the report and furnish him or her information on how to contact the agency which furnished the report. FCRA does not require the employer to accept an applicant’s claim that the report is false, or to wait any specific amount of time to fill the position while the applicant contests the report.

Berkowitz: There are new significant developments expanding the rights of whistleblowers. In March 2014, in Lawson v. FMR LLC, the Supreme Court ruled in favour of granting broad whistleblower rights, under the Sarbanes-Oxley Act of 2002, to lawyers, accountants, investment advisers – and indeed, any other individual who is employed by a third party to provide services to a publicly traded company. Sarbanes-Oxley prohibits a public company, “or any officer, employee, contractor, subcontractor, or agent of such company”, from discharging, demoting, suspending, threatening, harassing or in any other manner discriminating against “an employee” in the terms and conditions of employment, because of whistleblowing or other protected activity. The Court held, “Legions of accountants and lawyers would be denied [Sarbanes-Oxley’s whistleblower] protections”, if Sarbanes-Oxley were not read to provide this remedy. Thus, it is not hyperbole to describe the decision as providing a sweeping new remedy for lawyers and accountants.

Oldham: The FCRA sets forth the permissible purpose guidelines for performing background investigations, and pre-employment is one of them.

RC: What is the significance of the new guidance on background checks, published by the US Equal Employment Opportunity Commission (EEOC) and the Federal Trade Commission (FTC)? What is the purpose behind the publication of this guidance?
**Berkowitz:** The new guidance signals that these two federal agencies are looking anew at employer practices in this area and are prepared to enforce them as necessary. The EEOC’s principle concern is assuring that employers are not using background checks in a discriminatory manner. First, they want to be sure that, to the extent an employer uses background checks, it makes the decision to do so without regard to the applicant’s particular protected status, whether race, religion, age, national origin, and so on. Next, they want the business community to be aware that certain minorities may be more negatively affected by the use of background checks. For example, minorities may be more likely to have criminal records than non-minorities; they may not have had the educational advantages of non-minorities; and women may be more likely to have credit issues. Even if the employer corrects for these potential disparities, the EEOC does not want employers to take different decisions, depending on the results they get in these checks, based on the employee’s protected characteristics. Thus, for example, as the EEOC said, “if you don’t reject applicants of one ethnicity with certain financial histories or criminal records, you can’t reject applicants of other ethnicities because they have the same or similar financial histories or criminal records”. The FTC’s principle concern is assuring that employers comply with the federal FCRA, which imposes quite onerous requirements on employers who utilise background checks in their hiring practices. The entire procedure, from gaining consent to making a hiring decision, is regulated. Among other things, the employer must provide the applicant, or employee, written notice of their rights under the FCRA, on a separate form; it must provide them notice in the event that it learns information concerning the applicant that may cause the employer to make an adverse decision; it must offer the applicant a reasonable opportunity to review and potentially challenge the information; and it must provide separate notice to the individual if in fact an adverse decision is taken as a result of the information. So, the new guideline sends the clear message that these important federal agencies are flexing their muscles in this area.

**Wray:** The EEOC has taken the lead, and the FTC has assisted, in trying to get out the word of longstanding but often unrecognised EEOC policy. The EEOC is concerned that many employers have adopted background check policies which have a discriminatory impact on certain minorities, particularly African-Americans and Hispanics/Latinos. With over 700,000 persons getting out of US prisons each year, a large number of whom are minorities, the potential impact is significant, and it is evident that joblessness contributes to recidivism. It has long been the position of the EEOC that any policy which has an adverse impact must be job-related and justified as a business necessity. The EEOC does not claim that criminal background
EXPERT FORUM

CHECKS ARE UNLAWFUL, BUT STATE THAT ARREST RECORDS SHOULD NEVER BE USED TO DISQUALIFY AN APPLICANT, AS AN ARREST IS NOT PROOF OF A CRIME. An applicant may, however, be asked about the circumstances of an arrest, and any job-related information obtained from the inquiry may be considered. With respect to convictions, the EEOC warns that any policy which precludes hiring of any person ever convicted of any crime, or even of a felony, is very likely unlawful, as it will have a disparate impact and probably cannot be shown to be a business necessity. Instead, the EEOC counsels, an employer should consider on an individual basis the nature of the crime for which an applicant was convicted, the requirements of the job for which the applicant applies, and the time and conduct since the applicant was convicted or released from prison. Employers may apply a standard or matrix, for example “10 years since any conviction for theft for any position handling money”, but even then, the EEOC says, individual case by case consideration is required if the applicant cannot meet the standard. The EEOC has likewise claimed that credit checks may have a disparate impact on certain minorities and must therefore be job-related and consistent with business necessity. It has had difficulty sustaining this position in the courts, however, and one federal court of appeals recently accused the agency of suing a company “for using the same type of background check that the EEOC itself uses”. It noted that the EEOC personnel handbook recites that “[o]verdue just debts increase temptation to commit illegal or unethical acts as a means of gaining funds to meet financial obligations”. Because of that concern, the EEOC runs credit checks on applicants for 84 of the agency’s 97 positions.

The EEOC does not claim that criminal background checks are unlawful, but states that arrest records should never be used to disqualify an applicant, as an arrest is not proof of a crime.”

Oldham: This guidance simply echoes the guidance set forth by the FCRA. Being on top of regulatory compliance is essential.

Salins: In a first-time collaborative effort, the FTC, which enforces the FCRA, and the EEOC jointly issued guidance on 10 March 2014 on the appropriate use of background checks by employers when making hiring and personnel decisions. Although this is the first official federal insight on
this topic since the EEOC’s April 2012 guidance, it does not break new ground, but serves more as a reminder of employers’ existing obligations under the FCRA and federal-nondiscrimination laws. The agencies emphasise that employers need written permission from job applicants before getting background reports about them from third party companies that compile background information. They also reaffirm it is illegal to discriminate based on a person’s race, colour, national origin, sex, religion, age, disability or genetic information when requesting or using background information for employment. The fact that the EEOC and the FTC have collaborated to issue these guidelines reaffirm that both agencies consider this topic to be a priority and could potentially share information when enforcing laws concerning use of background checks.

Hale: In February 2014, the EEOC and the FTC published joint guidance on the use of background checks, with the EEOC focusing on avoidance of unlawful discrimination and the FTC focusing on compliance with the FCRA. The guidance was in two brochures—one for employers and the other for applicants and employees. The guidance broke no new ground. Instead, it described the basic requirements in plain language terms. At least on the surface, it appears that the purpose of publishing this guidance was to provide easily understood advice about implementing background checks, particularly when they disclose criminal record information. Certainly that is what the EEOC said. In its press release concerning the guidance, the EEOC said that the purpose was to provide “user-friendly technical assistance to our stakeholders”. It had been reported since the EEOC’s issuance of its guidance on the use of criminal records that the EEOC would be addressing the subject of the use of credit records in employment. It has not done so yet. Indeed, the joint guidance comments on the use of criminal records in employment decisions without addressing the use of credit records. As with criminal records, the case can be made that using credit records in employment decisions can have a disparate impact on members of minority groups. By the same token, many employers consider credit history to be an important factor in assessing applicants, at least for positions that will involve ready access to funds. It may be that the joint EEOC-FTC guidance was a preliminary step and that more potentially controversial guidance focusing on the use of credit records in employment decisions is still to come.

RC: How has the new guidance been received by the business community? What main criticisms have emerged?

Wray: The business community’s reaction has been mixed. Some larger employers, having dealt with the issue in the past, regard the new guidance
as ‘old news’, EEOC states, however, that the percentage of employers using the individualised assessment approach has increased from 32 percent to 88 percent in one year. A number of employers, both large and small, are concerned that compliance with EEOC’s position may put them at risk under some state laws which, for example, prohibit hiring of felons into a particular job. EEOC regards any such state laws as pre-empted, or trumped, by the federal laws it enforces. Another voiced concern is that the individualised assessment EEOC advocates could result in disparate treatment claims. Employers are also concerned about the ambiguity inherent in the ‘individualised assessment’ balancing act and fear that their good faith individualised assessments may be second-guessed. Moreover, many in the business community regard this guidance as yet another effort by the government to act as a ‘super personnel agency’ interfering in legitimate business decisions without statutory authority to do so.

Berkowitz: The concern of the business community is that the guidance does not take sufficient account of the legitimate need for employers to conduct background checks in an increasingly dangerous world. It also purports to set forth burdensome new so-called ‘requirements’ for employers in carrying out background checks. While the guidance does not have the force of law, the EEOC will certainly assess employers’ practices based on the extent to which the guidance is followed, and at least some courts may defer to the EEOC’s expertise and find them to have the force of law. Employers are also concerned by the EEOC’s
aggressive litigation in this area – the EEOC recently filed several lawsuits alleging that employers violated federal anti-discrimination law by implementing and utilizing criminal background check policies that resulted in employees being terminated and others being screened out for employment.

Oldham: The business community must be committed to being compliant with all guidance and regulations. We have not heard any criticisms as a result of work in the background investigations business.

Salins: The new FTC/EEOC guidance has been viewed as a clear and concise review of existing rules. Yet, the EEOC’s April 2012 guidance has been subject to severe criticism which is not addressed by the new guidance. In July 2013, Attorneys General from nine states sent a complaint letter to the EEOC, accusing it of unlawfully expanding the scope of Title VII to cover “former criminals” and urging it to reconsider its stance on background checks. In February 2014, the EEOC’s 2012 guidance came under fire by a report from the US Commission on Civil Rights, in which commissioners criticised the guidance as “deeply flawed” because it misapplies disparate impact theory. The EEOC has not been successful in litigations it has pursued in this area, most recently in EEOC v. Kaplan Higher Education Corp., in which the Sixth Circuit chastised the EEOC for using flawed methodology to try to prove use of credit checks as a pre-employment screen had an unlawful disparate impact against Black applicants. Despite the criticism and litigation losses, the EEOC has continued to defend its position on criminal background checks to date.

“\textbf{The business community must be committed to being compliant with all guidance and regulations. We have not heard any criticisms as a result of work in the background investigations business.}”

Jerry Oldham, 1stWEST Financial Corporation

Hale: Frankly, I do not believe that the EEOC-FTC guidance has led to any serious concerns or criticisms by the business community. The guidance simply summarises the applicable legal standards. I anticipate that if the EEOC issues guidance concerning the use of credit records in employment decisions, that will be scrutinised closely and may well lead to criticisms if it goes beyond established law.
RC: Could you comment on the relationship between state and federal anti-discrimination laws in the US? What similarities and discrepancies exist, and what challenges can arise from this for employers?

Salins: Many states and cities have anti-discrimination laws that provide greater protections than federal laws. For example, some state and local laws make it unlawful to discriminate based on political activities and legal recreational activities outside of working hours, so questioning applicants on those topics, or making decisions based on such activities revealed on social media sites, should be avoided. With respect to background information, a growing number of state and local governments – including Hawaii, Massachusetts, Minnesota and Rhode Island – have passed ban-the-box laws. These laws outright prohibit or severely restrict employers from asking applicants about criminal history in the initial employment application before either conducting an interview or making a conditional offer of employment. In addition, laws limiting employer use of credit history for hiring and personnel decisions are currently in effect in 10 states: Colorado, California, Connecticut, Hawaii, Illinois, Maryland, Nevada, Oregon, Vermont and Washington. Employers with operations in multiple states and localities that would like uniform employment policies may opt to comply with the law of the most restrictive jurisdiction in all locations.

Hale: In most respects, the substantive legal standards are the same. By the same token, the procedural standards and the standards concerning damages can make a significant difference. The most substantial substantive difference between some states’ laws and federal law concerns sexual orientation. There is no federal law prohibiting discrimination in employment based on sexual orientation. However, many states expressly prohibit employment discrimination based on sexual orientation. In some areas, different legal standards can apply within areas of discrimination that are prohibited by both federal and state law. For example, under federal law, an employer is not necessarily automatically liable for sexual harassment by a supervisor that results in a hostile environment, if the employer can establish certain defences and there has been no tangible employment action. In some states, however, an employer is automatically liable, without any opportunity to establish the defences that are available under federal law. Damages in employment discrimination cases can be significantly different, depending on whether a lawsuit is based on federal or state law. For example, damages for emotional distress and punitive damages are limited under federal law to caps of between $50,000 and $300,000, depending on the size of the employer. At
least in many states, no such caps exist. Moreover, if an employer and a plaintiff-employee are citizens of the same state and the employee sues solely under state law, the plaintiff-employee can file the lawsuit in state court and preclude the employer from removing it to federal court. Although courts and judges are far from uniform, the usual reputation of federal courts is that they are more probing in assessing whether there is a sufficient basis for a case to survive an employer’s motion to dismiss or an employer’s motion for summary judgment, either of which can result in dismissal without a trial. In short, on a day-to-day basis, differences between federal and state discrimination laws generally do not affect how an employer manages human resources or hires or supervises employees. However, once litigation is threatened or filed, the law that applies can make a difference in the potential consequences for an employer. Of course, in some other areas outside the discrimination law arena, such as overtime pay and leaves of absence, there can be significant state-by-state variations and significant differences between state and federal law. Those differences can result in increased complexity for employers managing multistate operations.

Oldham: State and Federal anti-discrimination laws have existed for a very long time. Again, compliance is the key.

Berkowitz: Federal anti-discrimination laws establish a baseline for employers, but many states and municipalities provide protections that go well beyond federal laws. There are a number of key differences. In terms of disability discrimination, the definition of ‘disability’ is often far broader under state law than under the federal ADA – thus, for example, an employee or applicant who is suffering a passing illness might not be disabled for the purposes of the ADA, but may be under New York State or New York City law, and the employer may have a legal obligation to make a reasonable accommodation to the individual, who might also be protected against adverse employment decisions based on the disability. In terms of sexual orientation discrimination, federal anti-discrimination law does not explicitly prohibit employment discrimination based on sexual orientation, the laws of many states and municipalities do prohibit this. For example, in New York, the law prohibits discrimination based on actual or perceived sexual orientation – heterosexuality, homosexuality, bisexuality or asexuality. Regarding age discrimination, the federal Age Discrimination in Employment Act (ADEA) prohibits discrimination only against individuals who are age 40 or over, and the law generally is intended to protect older individuals from discrimination in favour of younger individuals; but state laws may be closer to the UK model, and simply prohibit discrimination on the basis of age, so long as the individual is aged 18 or over, and regardless of
whether the discrimination is based on relative age or relative youth.

Wray: Employers in the United States must comply not only with federal law, but with state law and local ordinances, at least to the extent that state and local legislation does not contravene federal law. Discrimination on the basis of sexual orientation is often cited, as it is not currently prohibited by federal law, but it is prohibited in many states, and by many local ordinances. Most states have their own human rights agencies, which may have different procedures and notice posting requirements. Minimum wage and overtime requirements more stringent than those of the federal government are permitted and exist in many states. Additionally, some states, including California, Illinois, Connecticut and Maryland, prohibit the use of credit information by employers unless certain exceptions apply. Keeping up with these varying requirements can be a challenge to companies. That said, most employers are able to operate the same way across the nation with respect to their dealings with employees. Few employers of any size discriminate on the basis of sexual orientation or marital status, as examples, regardless of whether such discrimination is prohibited in a particular jurisdiction. Likewise, with the exception of California and Montana, absent agreement between an employer and employee, employment in the United States is ‘at will’, meaning that either the employer or the employee may terminate the relationship without notice or cause for any or no reason unless the reason is one prohibited by law. No prudent employer in any state would sack an employee without a legitimate reason, however, since it may be called upon to justify itself in the face of a discrimination, whistleblower, or other claim.

“Federal anti-discrimination laws establish a baseline for employers, but many states and municipalities provide protections that go well beyond federal laws.”

- Philip Berkowitz, Littler Mendelson

RC: What steps can companies take to reduce risks arising from new employees yet still comply with state and federal employment laws? What policies and procedures should they implement?

Oldham: With regard to what we do, employers should require that each new prospective employee
**EXPERT FORUM**

**SIGNA0RE
%MPLOYMENT2ELEASEAND!UTHORISATION**

&ORM GIVING PERMISSION FOR THE EMPLOYER TO
HIRE A BACKGROUND INVESTIGATION TO VERIFY ALL
INFORMATION IN THE EMPLOYMENT APPLICATION AND
PERFORM ADDITIONAL INVESTIGATIONS, INCLUDING MEDIA,
civil and criminal litigation history, judgments, tax
liens and bankruptcies.

**Berkowitz:** Companies need to be very careful
that they are retaining employees as employees
and not as consultants or independent contractors.
If the individual is reporting to work at set times, to
a particular individual, and taking direction; if the
individual is performing work to the standards of the
company; if he or she must report to the job and
does not have the discretion to send a replacement
– as might happen, for example, if you retain a
painter or carpenter to work on your house; if the
individual has a company desk or office, and is given
a company phone or email address, and a business
card; if the individual does not have a separate
corporation to which you are writing the cheque;
then the individual is likely to be considered to be
an employee and not a contractor. Companies need
to be very sure that they properly classify new hires
as either exempt or non-exempt from the federal
and state laws mandating payment of overtime. This
requires a careful analysis of their job duties. Getting
it wrong can result in liability for unpaid overtime
wages for up to three years, plus liquidated damages
and attorneys’ fees. These cases are most frequently
brought as collective actions – a ‘class action’ hybrid
– and so they are extremely costly, and liability of
often off the charts. Companies need to standardise
hiring practices and provide training to managers
as well as human resources professionals who are
involved in the process. Of course, employers also
need to be sure that those making hiring decisions
are not asking candidates unlawful questions, such
as those dealing with pregnancy, maternity leave,
marital plans, retirement plans, childcare and other
hot-button issues.

**Wray:** Despite the hurdles erected by federal
agencies, background checks of applicants remain
a valuable tool for avoiding hiring of untrustworthy
or potentially violent applicants. Additionally, the
information submitted on applications should be
carefully checked and each applicant carefully
interviewed. Of course, inquiries which elicit
disclosure of racial or ethnic status or religion should
be avoided. Where a company uses an outside
agency to verify applications, the agency should
be one that does not report medical information or
employment-related litigation to the company even
if it is volunteered by the applicant. It is wise to have
a written instruction to, or a written verification from,
the agency to that effect. Companies should not
only learn the applicable law when first going into
a jurisdiction, but should make regular updates a
priority. Employer associations, human resources
professional associations and law firms are good sources of information.

**Salins:** Conducting background checks on prospective employees is good practice to keep the workplace safe, protect the company’s assets and avoid negligent hiring claims. Employers who rely on background checks should familiarise themselves with the EEOC’s April 2012 enforcement guidance, and re-examine their procedures in light of such guidance. For example, employers are advised to: only ask for information relevant to the duties of the position; when a credit report or criminal background check reveals issues, do an individualised assessment by informing the applicant he or she is being excluded because of an unfavourable report, and providing the applicant with a chance to explain the credit report or criminal background check; and justify any exclusion based on criminal history in light of the nature of the crime, the time elapsed and the nature of the job. Furthermore, employers should ensure their procedures comply with applicable state and local laws that restrict the type of background information employers may solicit from an applicant.

**Hale:** First, make sure to have a rigorous and systematic process for considering applicants. Use reference checks and background checks. Also use social media, but do not engage in deceptive practices and be careful not to use information that cannot be considered. Second, have all applicants sign an employment application. That helps to ensure the receipt of consistent information concerning applicants. In addition, the employment application can be a useful vehicle for obtaining an acknowledgment of the at-will nature of employment and obtaining an authorisation of background checks for FCRA purposes. Note that a separate sheet notifying applicants of the possibility of background checks also needs to be provided. The employment application can also include an agreement by applicants to waive any claims associated with providing references. Such a waiver can be useful in encouraging possible references to provide reference information. Third, train employees who are involved in interviewing and selecting employees on what are permissible considerations, what are impermissible considerations and what traps to avoid in conducting an interview. Fourth, ensure that there is a systematic documentation process. That includes obtaining and preserving I-9 forms and managing employment-related agreements, including countersigning agreements. Finally, as should go without saying, have a comprehensive equal employment opportunity policy, including the provision of reasonable accommodations in the hiring process, as well as during employment

**RC:** What final advice can you offer to companies on minimising and mitigating
employment risks associated with potential new employees?

Hale: Do not skimp on the investment in the hiring process. Make sure to cast a wide net. That will maximise the likelihood of bringing in the best candidates. It will also help in developing a diverse applicant pool. Then be probing in the process, focusing on the skill sets of prospects and obtaining information from a variety of sources. Many lawsuits by terminated employees are the ultimate result of a poor hiring process. Establishing a comprehensive and systematic process and implementing it rigorously is an employer’s best means of avoiding employment litigation and hiring the most effective workers.

Salins: Engaging third parties to conduct background checks is a good approach to avoid obtaining applicants’ protected class information but, given the high stakes litigation in this area, employers should be sure to comply with all requirements of the FCRA and similar state laws when doing so. While employers face the task of deciding whether to screen for applicants’ criminal histories and face the risk of an EEOC enforcement action or whether to hire individuals with criminal backgrounds and face lawsuits alleging, for example, negligent hiring claims, the continued failure of the EEOC to succeed in these lawsuits leaves this an area of continued uncertainty. Employers are advised to stay abreast of any new guidance issued by the EEOC, new state and local laws pertaining to criminal records and credit reports and other developments in this area.

Wray: Companies may wish to watch the ‘ban-the-box’ movement, which refers to the fact that inquiries concerning convictions are often in a box on employment applications. Eleven states and over 50 cities and counties have enacted laws that require public or private employers to postpone an inquiry concerning criminal convictions or a background check until after a tentative hiring decision has been made. The theory is that this will give job-seekers the opportunity to be reviewed on
their qualifications first. If an employer is required to adopt or voluntarily adopts such a policy, it should avoid any temptation to make the inquiry or conduct the background check at the same time it asks for medical information, as there must be a conditional offer of employment contingent solely on the medical review before a medical inquiry lawfully may be conducted.

**Berkowitz:** Companies need to recognise that we do things differently in the US. We are well known for our ‘employment at will’ concept, but many foreign employers misconstrue the term, and believe that it’s permissible to fire someone with no reason at any time. Employers may also feel that this doctrine reflects a general *laissez faire* attitude on employment practices in the US, but nothing could be further from the truth. US hiring and employment practices are highly regulated, both by statutory law, which may be federal, state or local, and by common law. As a result, an employer doing business in the US needs to consider what may be highly divergent employment law requirements, depending on where the business is established. At the end of the day, though, employers do thrive in the US. Employers need to put in place policies that make clear what their practices are, and that reflect legal requirements. Many laws pose specific requirements at the time of hire, including in particular the prohibitions of non-discrimination laws, the stringent requirements of employee classification laws, and myriad employee notice requirements. Employers who take the time to engage professional assistance, who hire knowledgeable human resources executives, and who provide training to all employees on their rights and responsibilities under US law, can navigate our system with great success.

**Oldham:** Companies should hire an outside competent firm to do a thorough background investigation of each new hire prospect, regardless of their ranking within the organisation. **RC**
COMMUNICATING THE CYBER CRIME THREAT TO THE UK’S C-SUITE

BY MIKE GILLESPIE AND ELLIE HURST
> ADVENT IM LTD

The UK is developing a keen focus on cyber crime but will it be sufficient to push cyber security into the boardrooms of UK plc in time to mitigate the growing cyber risk? We think we know what has to be done but the cyber crime data we have to work with in assessing this risk is flawed in many ways. This is a potential stumbling block in effectively communicating the threat to our nation’s C-suite.

UK plc has taken a tough stance on cyber crime. Positioned at the leading edge of tackling this global threat, the UK is affiliated with all the right people to help move the global response forward, such as Five Eyes Alliance, the EU, G8 cybercrime working groups, Europol and Interpol. Andy Archibald, Head of the National Crime Agency’s (NCA) National Cyber Crime Unit (NCCU), has a keen focus on driving improvement in this vital area. But in the UK, our ability to fully grasp the scale and cost of cyber crime could be hampered by the quality of the statistics available, if a research report from the Home Office is correct. How cyber crime is reported (or not), prosecuted and therefore reported back to the public, is inconsistent and unreliable. This patchy understanding does not help us when it comes to strategising response and mitigation and could potentially lead to assumptions and the unintended consequence of actually creating more risk. We do not know the real scale of cyber crime nor do we have an accurate picture of what it is costing.
us every year. Current estimates run between £15bn and £28bn. Given that kind of scale, it seems whatever the actual figure, it probably looks more like a telephone number.

In October 2013 the Home Office released, ‘Cyber Crime: A review of the evidence’ by Dr Mike McGuire and Samantha Dowling. This was a serious study of online behaviour and crime and some of the key findings will resonate but probably not surprise those working in risk and security. Indeed, it underlines issues many of us have been talking about for a while. Several issues present themselves from this study – underreporting and confusion about how to report cyber crime, a lack of understanding of what cyber crime is, and the lack of clarity in terms of detection and prosecution of ‘cyber’ crimes and not traditional crimes.

Broadly speaking, we are talking about two different kinds of crime: (i) ‘cyber-dependent’ crimes, which could only be committed using a computer, networks or other form of ICT; and (ii) ‘cyber-enabled’ crime. Cyber-dependent would be crimes such as spreading malware, hacking and Distributed Denial of Service (DDoS) attacks. From a business perspective that could be a DDoS attack, when the criminal ‘pings’ a server many thousands of times from many different locations, causing the server to crash and their network or website to be unavailable. Both of these attacks are dependent upon cyberspace. The emergence of fake anti-virusware that is actually a Trojan is a new and extra cynical plot twist in this kind of crime. Hiding in plain sight, this sort of Trojan does the job it actually claims to be protecting you from. Overall, the report found that individuals and businesses in the UK were confused about cyber-dependent crime. In fact, the figure quoted was 2 percent of online crime incidents were reported
to the police. But as the police do not as a whole distinguish between online and offline crime, we are struggling to get our arms round what the landscape really looks like. More people arrested for this kind of crime actually get prosecuted under the Fraud Act than the Computer Misuse Act and so we have no way of knowing if cyber crime is costing us more, costing us less, growing or declining. Cyber-enabled crime is different and this may be where people’s confusion grows. A traditional crime such as fraud may have a cyber element to it, such as ‘phishing’ to steal from an individual – the emails we all get from time to time, purporting to be from our bank asking us to login using the link. An individual could lose their savings or have their identity stolen through a phishing attack. Of course, businesses also receive phishing attacks, but both individuals and businesses do not always perceive they have been a ‘victim’ if their losses are refunded by their bank. Action Fraud stated back in 2012 that there were over 51,000 UK bank phishing sites; it seems unlikely that number could have decreased over the following two years.

Geography is another issue that changes when we consider the difficulties or confusion around cyber crime of all types. If an individual is mugged in a car park or in the street, the victim and the perpetrator share geography, there is no question of where the crime occurred. If you get mugged or attacked online by a cyber criminal, where did the crime occur? Was it in the victim’s home or workplace, if it happened to a business was it in the place where the employee was or was it head office? Was the location of the crime wherever the criminal was? If that was the case this could be anywhere in the world, so to whom should the crime be reported and how? So, yet another layer of inconsistency and confusion is added to an already complex and highly toxic set of issues.

Crime has moved on quickly and its detection and prosecution has not kept pace – is that the conclusion we are to draw?

“Crime has moved on quickly and its detection and prosecution has not kept pace – is that the conclusion we are to draw?”
the National Cyber Crime Unit (NCCU) of the fairly recently established National Crime Agency (NCA). It is clear that the police take cyber crime very seriously and are going to great lengths to tackle cyber criminality but given some of the issues we have discussed here that have arisen from the Home Office report, the challenge is a steep one. Also we are still talking about police who are used to investigating and prosecuting ‘traditional’ crime. There is a tendency within police for officers to move around every two years which is another layer of challenge to a consistent approach that will also need to be addressed if the NCCU is going to have the best possible chance of success.

It seems that, one way or another, the police have been trying to get their arms round cyber crime for almost 15 years. It is possible that more support from the private sector – to get the expert help – will help realise the potential of the NCCU. Having said that, the skills shortage in the cyber security world is pronounced (as the recent recruitment push through initiatives like UK Cyber Challenge shows) and set to get worse, so an additional issue may be in hoping that private sector experts are prepared to work with public sector pay-scales and structure. Whatever they decide to do to mitigate the growing threat from cyber space, they need to think quickly. Through the ‘internet of things’ experts predict another 75 billion internet enabled devices will enter the ether over the next three years. From TVs to fridges and internet enabled spectacles, the world is going to be living far more of its life online – along with the cyber criminals, of course.  

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

Ellie Hurst
Marketing & Communications Manager
Advent IM Ltd
T: +44 (0)121 559 6699
E: ellie.hurst@advent-im.co.uk
MINI-ROUNDTABLE

MANAGING RISK AND SECURITY ISSUES ARISING FROM MOBILE ACCESS
PANEL EXPERTS

Mark W. Brennan
Partner
Hogan Lovells US LLP
T: +1 (202) 637 6409
E: mark.brennan@hoganlovells.com

Mark Brennan’s practice encompasses communications and consumer protection, with a particular focus on the legal frameworks applicable to digital and mobile platforms, international telecommunications regulation, and mobile financial services. Mr Brennan has substantial experience assisting clients with complex consumer protection issues that span multiple fora, including the Federal Communications Commission (FCC), Federal Trade Commission (FTC), NTIA, Congress, state authorities, and state and federal courts. He represents clients on a wide array of regulatory and commercial issues related to the Telephone Consumer Protection Act (TCPA) and telemarketing issues, telecommunications licensing, mobile applications and location-based services, spectrum policy, equipment development, and data privacy and security matters.

Tara N. Cho
Associate
Poyner Spruill LLP
T: +1 (919) 783 1079
E: tcho@poynerspruill.com

Tara N. Cho is an attorney in the Poyner Spruill Privacy and Information Security Practice representing clients across industry sectors including health care, clinical research, retail, technology, and financial services. She is a Certified Information Privacy Professional for both the US and Europe and advises clients on a range of issues to help them implement innovative and comprehensive compliance solutions.

Meighan E. O’Reardon
Senior Associate
Pillsbury Winthrop Shaw Pittman
T: +1 (202) 663 8377
E: meighan.o.reardon@pillsburylaw.com

Meighan E. O’Reardon is a senior associate in the law firm’s Global Sourcing practice in the Washington DC office. Ms O’Reardon also regularly advises on data use and privacy matters. Her data privacy and security experience involves counselling clients on matters related to data breach response, privacy policies and terms of use, international data transfer of personally identifiable information, and the creation of privacy and security compliance programs. Ms O’Reardon also advises on key privacy and security contract terms. Her works on mobile technology and social media matters including the creation of social media policies, bring your own device terms, and other mobility issues.

Cheryl Tang
Senior Manager, Mobility
Symantec
T: +1 (650) 527 3992
E: cheryl_tang@symantec.com

Cheryl Tang is a Senior Manager, Mobility at Symantec. She is a seasoned marketing professional with broad experience in product marketing, outbound marketing, messaging and positioning, strategy and sales.
RC: Could you outline the recent influx of mobile and personal devices used in the workplace? How is this trend blurring the line between work and home life?

Brennan: The ubiquity of mobile devices has started blurring the line between work and home. For example, International Data Corporation (IDC) predicts that 175 million workers globally will bring their own smartphones to work by the end of 2014, and that number will reach 328 million by 2017. These activities create some risk for both organisations and individuals, as the norms that govern our personal and work lives do not always align. For example, when an employee communicates with friends and family via social networks and messaging apps using the same device that is used to access the employer’s proprietary information, there is a risk that the employee will use the device in ways that fail to meet work norms or expose the employer’s information to unnecessary risks. These actions create potential security incidents that can threaten an enterprise.

O’Reardon: The use of mobile devices that serve a dual function for business and personal use are nearly ubiquitous in the workplace. Using personal mobile devices at work has become so common that BYOD can no longer be treated as a mere trend. A recent Cisco study found that 90 percent of full-time American workers use their personal smartphones for work purposes. Use of BYOD has made 24/7 access to business communications virtually seamless but raises significant privacy considerations regarding the extent to which employers may control and access content on personal devices. The use of BYOD can also raise significant employment issues – especially in the non-exempt/hourly context. From a corporate standpoint, this highlights the importance of having clear, practical and defined rules and policies in place related to BYOD.

Cho: The obvious risks are security breaches and data loss, such as losing an unencrypted device with locally-stored proprietary or personal information. There also are compliance risks, particularly in highly-regulated industries such as health care and finance, in which BYOD solutions must meet the security standards required by applicable regulations. Regarding use of work-based wireless networks, authorising employee-owned devices will necessitate changes to – and likely complicate – the task of monitoring that network’s use by potentially unauthorised devices, and employing an appropriate degree of location or communications monitoring without violating employee privacy rights. Perhaps the most difficult challenge is changing employees’ mindsets. Employees think of the device as their property, but must understand and agree to turn
the device over for inspection if necessary in a legal dispute or security breach, quickly report to the company if the device is lost or stolen, maintain security safeguards, and avoid high-risk practices such as cloud back-up or continuous use of Bluetooth-discoverable mode.

**Tang:** A recent Yankee Group study found that 60 percent of companies allow consumer devices and software in the workplace, up from 43 percent in 2011. The lines between work and home life have definitely blurred. Employees’ desire for flexibility coupled with the convenience of mobile devices and apps are fuelling the BYOD trend. While BYOD has often increased productivity, it has also introduced new and evolving security challenges. We strongly advise that enterprises develop a strong BYOD plan and invest in solutions that go beyond simply managing devices. Rather, enterprises should seek solutions that allow for the protection of corporate data without impacting personal apps and data or infringing on employee privacy.

**RC:** What specific security issues arise from the use of personal devices, including their integration with work-based wireless networks?

**O’Reardon:** On the one hand, personal devices are like any other device attached to the corporate network, so there is no material change in risk profile as compared to any other network attached device, such as a laptop. On the other hand, there are significant implications given the portability of mobile devices and the way in which we use them in our daily lives. In fact, your young children may be one of the most serious security threats because they know how to unlock your smartphone and unwittingly access corporate emails and applications. More seriously, because of the personal control over smartphones and tablets, employees can easily disable security features, allowing direct access to corporate email and other systems that are connected to the device, if the device is lost or stolen.

**Tang:** There are many challenges associated with BYOD. The more devices connected to a network, the harder it becomes for a business owner to track and manage data. These additional devices also create more points of entry for cyber attacks, as the security posture of the devices may not comply with corporate standards. Users are also less aware of the security risks associated with mobile devices and apps. According to the 2013 Norton Report, nearly 50 percent of users do not take basic precautions such as using passwords or security software. Personal devices with sensitive information can be lost or stolen, putting enterprise data at risk.

**Cho:** The obvious risks are security breaches and data loss, such as losing an unencrypted device with
locally-stored proprietary or personal information. There also are compliance risks, particularly in highly-regulated industries such as healthcare and finance, in which BYOD solutions must meet the security standards required by applicable regulations. Regarding use of work-based wireless networks, authorising employee-owned devices will necessitate changes to – and likely complicate – the task of monitoring that network’s use by potentially unauthorised devices, and employing an appropriate degree of location or communications monitoring without violating employee privacy rights. Perhaps the most difficult challenge is changing employees’ mindsets. Employees think of the device as their property, but must understand and agree to turn the device over for inspection if necessary in a legal dispute or security breach, quickly report to the company if the device is lost or stolen, maintain security safeguards, and avoid high-risk practices such as cloud back-up or continuous use of Bluetooth-discoverable mode.

**Brennan:** Personal devices can introduce significant risk into an organisation’s security program. Each device introduces a potential new attack vector for the organisation’s network, systems and applications. It also represents a new potential means by which data can be inadvertently or maliciously removed from the organisation’s controlled environment. Gartner projects that by 2017, 75 percent of all mobile security breaches will be due to misconfigured applications – a particularly likely issue with personal as opposed to organisation-owned devices. Personal devices are often not subject to the same rules regarding asset tracking and monitoring that organisation-owned devices follow, which can make it more difficult for the organisation to manage such devices, respond to a potential breach or security incident involving a personal device – including a lost or stolen device – or assess the scope and scale of the impact of a security vulnerability or attack on the organisation’s network, systems, applications or data.

**RC:** To what extent, do you believe, are companies aware of the threat posed by mobile devices to data privacy and cyber security? What steps can they take to minimise vulnerabilities?

**Cho:** Companies increasingly recognise and prioritise security programs designed to prevent costly data breaches and protect valuable data, with special emphasis on mobile devices. Most have focused on lost or stolen devices and implement data loss prevention – such as blocking downloads – or encryption as a result. Those actions are helpful, but do not address some of the lesser-known risks, like the vulnerabilities introduced to network security by personal devices authorised on the network. To minimise risk, companies can implement comprehensive security programs...
that include a mobile device management (MDM) solution that allows remote wiping, as well as encryption, authentication, password requirements and other controls on the device. In addition, proactive monitoring and malware prevention may be enhanced on the company network to prevent unauthorised access by or through mobile devices. Finally, strong policies and training will make employees aware of the risks and their accountability for the security of their devices.

**Brennan:** Enterprise awareness of the specific privacy and security threats posed by mobile devices is steadily increasing, but so is the size and nature of the threat. Gartner projects that by 2017, attacks and exploits will be focused on mobile devices, such as smartphones and tablets, instead of traditional workstations. IT and security teams must consider what rules govern the use of personal devices on work-based networks, such as whether additional authentication is required, how devices are tracked and what security measures, such as passcodes and remote wipe capabilities, are required before personal devices are even permitted to connect. Use of MDM solutions, which support restrictions on access to data and allow organisations to enforce evolving security policies, remains the best way to reduce the risks to the organisation.

**Tang:** Mobile attacks have increased each year because of the interest in the wealth of information stored on personal devices, which includes enterprise data. Mobile malware grew to 275,000 in June 2013, a four-fold increase from June 2012. Companies need a clear and thorough BYOD policy to secure and manage their data. We recommend a multi-layer approach to mobility. While many companies have initially gravitated to MDM to control devices, it is critical they go beyond simple device management to a comprehensive approach that includes user and app access, data and app protection, and threat protection. It is also incredibly important that the mobile threat protection provide robust app behaviour and reputation insight because the mobile threat landscape is constantly evolving.

“Enterprise awareness of the specific privacy and security threats posed by mobile devices is steadily increasing, but so is the size and nature of the threat.”

Mark W. Brennan
Hogan Lovells US LLP
O’Reardon: Security management becomes much more difficult the less control an IT department has over the relevant data and hardware. BYOD by its very nature makes control a challenge. Many security breaches using BYOD result from inadvertent action. For example, sensitive information could be accessed by unauthorised individuals who are using a friend’s iPad or sensitive data may be inadvertently placed in a shared cloud folder. IT departments are employing a variety of tools and practices to prevent security breaches. Security tools including password protection, forced disabling of certain applications and remote wipe controls are just a few examples. A growing number of companies also rely on mobile device management (MDM) solutions to help manage their BYOD programs. Finally, having enforceable, and enforced, policies can help drive behaviour, as well as chill risky behaviour.

RC: In your experience, do employees place enough importance on enabling the security controls of their devices and adopting recommended practices? What steps should companies take to monitor, identify and discipline staff who ignore these controls?

Tang: In many cases the greatest security risk is the non-malicious, uniformed employee. A recent survey conducted by Ostermann Research reveals that 15 percent of enterprise employees believe they have ‘none to minimal’ responsibility to protect corporate data stored on their personal devices. It is critical that organisations not only continue to educate employees about mobile dangers and risks, but also seek solutions that safeguard the apps, data and devices that employees use to access corporate data. Business owners should have a system in place to monitor which devices have access to enterprise data. For smaller companies, this might be a security solution with a management portal. For a larger company, this could be dedicated IT personnel. All companies, no matter the size, should have clear information-management rules in place and actively

“It is always important to have policies in place that are practical to implement and that the corporation enforces.”

Meighan E. O’Reardon
Pillsbury Winthrop Shaw Pittman
communicate these rules to employees. Companies should also work to create an environment in which their employees feel like partners in protecting the business.

O’Reardon: Generally speaking employees do not place enough importance on implementing and following sound security practices related to their BYOD devices. Many of the commercially available solutions to help with mobile device management force employees to rely on certain security controls, such as locking idle devices, limiting access to certain content, and so on. However, corporate BYOD policies and practices must balance employee control and corporate security interests. A policy should not be unfair to employees, and employers should provide clear notice and obtain employee consent before implementing BYOD policies that impact employee’s privacy and require certain end-user behaviour to strengthen security. Furthermore, it is always important to have policies in place that are practical to implement and that the corporation enforces.

Brennan: Employee error is often cited as one of the main causes of internal IT security incidents. And it is not entirely surprising that employees do not always implement recommended security practices. Some employees may also view security as a roadblock to convenience, as implementing some security controls – like encrypting information or setting strong passwords to access devices – may stand in the way of the ready access to connectivity that mobile devices are designed to provide. Monitoring device usage can be an effective tool to mitigate the risk of employee error or misconduct, but monitoring and employee discipline should not be the only pillars of a device management program. They are reactive tools that detect and respond to incidents that have already occurred. Mobile device programs should instead integrate proactive measures that prevent incidents from occurring. For example, employers should engage with employees to learn about the tools that employees are seeking. And employers should implement robust, ongoing training programs that educate employees about the importance of security. By fostering a two-way engagement over mobile device security, employers can provide accessibility and connectivity while promoting security.

Cho: In our experience, some employees will deliberately deactivate or circumvent security controls if doing so increases convenience, functionality or processing speed. Many employees, given the option, forgo even basic passwords. This general lack of willingness to choose security over convenience accentuates the need to implement an MDM solution so that security measures can be updated or confirmed using centralised, technical distribution and control that prevents employee modification. Absent such a solution, employers are
completely dependent on employees to maintain the security of the device, relying on policy, manual monitoring of compliance, and enforcement. The latter approach is resource-intensive, privacy invasive and legally risky. Under either approach, it is important to implement guidelines related to employer monitoring and sanctions policies so that employees are aware of enforcement and repercussions, and to train applicable staff, such as IT security and human resources, on these policies.

RC: What advice can you give to firms on drafting and implementing specific Bring Your Own Device (BYOD) policies throughout their organisation?

Brennan: An essential feature of any BYOD policy is transparency. That means that employers should ensure that employees understand both what the BYOD policy requires of them and why the policy is important. Unless employees buy in, the policy provisions ultimately may not be effective. In striving to address the security issues raised BYOD policies, employers should be careful to not turn a blind eye to employee privacy. Monitoring will likely be an essential element to any BYOD program, and monitoring implicates privacy. Employers should also take steps to ensure that their BYOD policies are appropriate for global implementation. For example, mobile devices can travel globally. Employee notice and consent may be sufficient to permit robust monitoring in some jurisdictions, but other jurisdictions may place strict limits on monitoring even if employees consent.

Cho: Implementation of a BYOD program means companies must transition from command-and-control mobile device frameworks for company-owned devices with company-controlled security to a program in which that control is relinquished, to varying degrees depending on the program, with greater reliance on policies and training. Developing strong terms of use and program policies are critical components of any BYOD program. Terms should make clear the employees’ responsibilities and acceptable use. Policies should include appropriate messaging regarding participation as a privilege that comes with obligations. Examples of focus areas to cover in these documents include the scope of the program, such as which employees can participate, what devices are allowed, applications that are acceptable, and so on; collecting and maintaining employees’ agreement to the terms of use; acceptable use and rules of conduct, including reporting lost or stolen devices; minimum security requirements for the device; and updates to the company’s affected security and privacy policies.

O’Reardon: Today implementing and managing a BYOD policy is not an option; it is an imperative. There are a number of best practices for designing an effective BYOD policy and compliance program.
First, a policy should be legally enforceable and realistic. Consider managing, but not prohibiting, activities that employees are almost certain to engage in. Second, collaborate horizontally within your organisation when designing a BYOD policy. Include stakeholders from legal, IT, and HR departments. Third, ‘one size fits all’ does not apply to BYOD programs. Policies should take into account the unique risks and regulations within an industry. In certain cases policies could be tailored to fit divisions or locations within a corporation. Fourth, explain specific employee obligations, and guide employee privacy expectations with plain-English rules and examples. Do not forget to keep good records of notification and consent. Finally, as with any policy, a BYOD policy will only be effective if continually enforced. An unenforced policy may prove worse than not having a policy at all. This means that ‘punishment’ needs to be tuned to be enforceable – that is, it is unlikely that a policy whereby employees who disable password protection are fired will be enforced. However, having a policy where employees who disable passwords are locked out of the network for a certain period may well be enforceable and drive the desired behaviour.

**Tang:** Companies should develop a written policy and communicate the guidelines to employees. There are a number of good places to start. Determine which devices you will support – tablets, iPhones, Androids, and so on. Determine what employees must do to access enterprise data on their personal device, including password protection and antivirus protection. Your company’s current PC policy is a good place to start. Determine policies around app use, downloads, and so on. Determine how you will support these devices: with a helpdesk, a dedicated IT person, or some other solution. Determine how you will manage devices. Some security suites come with a management portal; in other instances, IT personnel can help business owners track enterprise data on personal devices.

**RC:** In what ways do the risks arising from BYOD schemes differ between regions and industries? For example, how
might implementing a BYOD program in the US healthcare sector compare to implementing a BYOD program in the EU financial services industry?

O’Reardon: In terms of geography, certain countries, such as those in the European Union, have a much stronger approach to protecting privacy and a view that employee consent for a corporation to access content on a personal device may not be enforceable as it is coerced through the employment relationship. Thus, the use of policies to ‘give up’ privacy rights – such as agreeing that the company can review any and all information on a BYOD device – is less likely to be enforceable in Europe than in the United States. In terms of industry, the more sensitive the information or degree of regulation around data in that particular industry, the more risk involved in permitting use of BYOD devices to conduct business. If, for example, an entity places protected health information on mobile devices, that entity may want to think long and hard about whether BYOD devices should be used or whether such data may only be accessed on a corporate owned device. In some industries, use of personal devices for business purposes faces too many policy and legal hurdles to make the value proposition worthwhile.

Tang: Companies in industries with strict compliance laws, like healthcare and legal services, have to be particularly careful about tracking and managing sensitive information. There may be significant financial penalties if these highly regulated industries fail audits or experience data breaches. Privacy laws are also a factor, as some regions have strict privacy laws that create additional challenges related to implementing BYOD programs. In some cases, companies in these sectors have forbidden or restricted the use of personal devices in the workplace. Regulations vary from industry to industry and region to region.

Cho: The legal regimes relevant to BYOD vary greatly across geographic regions and industries, which can cause privacy and information security compliance programs to constrain global data flows if not approached practically. For example, a BYOD program in a US-based health care or financial company would implicate more compliance obligations than the same program in the retail industry, necessitating a more aggressive system of employee monitoring to combat security and legal risk. By contrast, in other regions, privacy is a fundamental right and related compliance is less disparate by industry. The aggressive monitoring considered necessary in some US compliance schemes may be illegal or subject to prior approval by labour rights representatives. Those differences must be navigated and incorporated into a global BYOD program, and sometimes result in a distinction between the types of data and applications...
employees in various regions will be entitled to access via a BYOD-enabled device.

**Brennan:** Organisations in certain regulated sectors and countries operate under a legal framework that may already govern BYOD schemes. For example, HIPAA governs the privacy and security of protected health information (PHI). A BYOD program can introduce new risks to PHI that must be considered and managed, with appropriate safeguards in place for the organisation to meet its privacy and security obligations.

**RC:** What legal and regulatory developments have you seen concerning the use of mobile and personal devices in the workplace? How are companies responding?

**Cho:** Security breaches continue to stay on the forefront of privacy and security developments, driving new legislation, aggressive security measures and corporate priorities in terms of mobile device management. In the US, employment laws are increasingly protecting employee social media accounts and location privacy has become a more prevalent concern. Globally, there are more comprehensive privacy regimes both emerging and expanding, perhaps most notably the proposed data protection reforms in the European Union. These laws typically are very protective of employee rights, particularly in personally-owned devices and personal communications. Reforms underway now promise ever-larger monetary penalties and greater compliance burdens in the privacy space. In short, laws and enforcement in this space have increased dramatically and it is certainly challenging for companies to stay in front of these changes. We have observed increased engagement of both privacy and security professionals internally as one response, and increased reliance on insurance as another.

**Tang:** Companies in industries with strict compliance laws, like healthcare and legal services, have to be particularly careful about tracking and managing sensitive information. In some cases,
companies in these sectors have forbidden or restricted the use of personal devices in the workplace. The US government issued a BYOD toolkit for federal agencies in 2012. Related to this, companies should also be mindful of employee privacy while monitoring activity on personal devices.

**Brennan:** Thus far, regulators have largely sought to govern the use of mobile and personal devices in the workplace with existing laws and regulations, rather than push for new mobile-specific authority. For example, the FTC has been focused on issuing guidance highlighting the specific risks and concerns surrounding mobile and personal devices in the workplace, as well as the significant security concerns involved in mobile software development. In July 2013, the FTC entered into a consent order with a major mobile device manufacturer based on allegations that the company had shipped devices with inadequate security and failed to employ reasonable and appropriate security practices in the design and customisation of its software on its mobile devices. For their part, companies are recognising that their workforce monitoring programs now may have global reach, as employees take increasingly mobile devices with them for travel and stay connected to the workplace from around the globe. Organisations are therefore re-evaluating their monitoring practices and workforce disclosures to stay within the confines of laws across the globe.

**O’Reardon:** Most federal and state regulations do not apply explicitly to BYOD practices, however, BYOD practices may exacerbate the risk of noncompliance with existing laws related to mobile technology and data security. Many of these laws were created to prevent unauthorised access to third party personally identifiable or sensitive personal information and require certain breach notification policies and other incident response procedures, which may be much more difficult to manage when employees do not report promptly the loss or improper access to personal devices. The application of other laws to the BYOD context may not be immediately obvious. Export laws,
such as the Export Administration Act regulate the carrying of certain information outside of the United States, or exposure of this information to certain foreign nations. Most significantly, employment practices have received the most scrutiny related to BYOD use. For example, violations of the Fair Labor Standards Act and other labour laws may be violated if non-exempt employees are explicitly or implicitly required to access and reply to emails outside of clearly defined working hours. Companies should be mindful of the legal considerations particularly related to data security, privacy and employment when drafting their BYOD policy. Including provisions in BYOD policies and implementing practices that address the applicable law in these disciplines is crucial.

O’Reardon: As BYOD has become the new normal, corresponding risks must be understood and mitigated against. Social expectations and norms are still evolving between employers and employees. Technological solutions, such as MDM services, are being developed and refined as well. Within this new and rapidly changing world the most important step that all companies should take today is to draft, enforce and communicate BYOD policies that can grow and change as smart devices continue to evolve. Note that we do not advise avoiding BYOD, except in certain industry sectors – rather, we advise being smart about how you embrace BYOD so that you can reap the benefits while minimising risk.

Brennan: Do not treat security trainings, BYOD policies or mobile device management programs as one-off initiatives. Mobile technologies and risks are evolving at a rapid pace, and training, policies and programs will have to evolve with them. Employers must keep abreast of the latest legal and regulatory changes in this area. And in working to manage mobile risks while respecting employee privacy, employers should remember that privacy and security are multifaceted, community issues that cannot be protected in isolation. Employers and employees are connected to complex ecosystems comprised of customers, service providers, suppliers, consumers, friends, family and others. If one part of the ecosystem is compromised, that can impact every participant. Employers must therefore

RC: With the use of smart devices set to become ubiquitous in the coming years, what final advice can you give to firms on managing mobile risks now and in the future?

Tang: Mobile devices and apps aren’t going away, so folding them into the workplace will increase productivity if done right. Enterprises can reap the benefits of mobility by developing smart BYOD plans and implementing a multilayer approach that includes user authentication and access, device management, app and data protection, and threat protection.
look outside their own organisations to evaluate leading practices and identify potential risks.

**Cho:** Security professionals and lawyers often make the mistake of comparing risks posed by a BYOD program to the perceived, ideal security environment reflected by company policy, assuming substantial compliance by the workforce. That comparison often makes BYOD look riskier by comparison, but ignores the reality that employees increasingly ignore or subvert the enterprise’s current security program by using unsanctioned personal devices, cloud storage and readily-available unsecured wireless networks for work. Numerous surveys report that most employees engage in these behaviours whether or not permitted by the employer. To make a smart choice about BYOD programs, organisations must acknowledge and evaluate the true information technology environment that comprises their ‘workplace’ and whether it includes use of unsecure mobile devices and associated networks and storage. If it does, a BYOD program may be a viable solution that can actually improve rather than complicate compliance and reduce rather than exacerbate risk. **RC**
The need for compliance and risk managers to understand data breach planning and response is important from start to finish.

In today’s environment, consumers have become more familiar with the reality and impact of data breaches than ever before. The surge in data breaches on the public radar has made a significant impact on consumer attitudes and expectations of businesses, with 62 percent of consumers having received more than one data breach notification involving separate incidents in the last two years (Ponemon Institute, The Aftermath of a Mega Data Breach: Consumer Sentiment).

With this comes what we have coined data breach ‘fatigue’. The Ponemon Institute research found the increase in data breach notifications and related media coverage has caused consumers to possibly become more apathetic. The increase in consumer notification is profound – the number of consumers who reportedly received a data breach notification doubled in 2013 compared to 2012. But, rather than taking action to protect themselves after a data breach, consumers are giving less attention to the severity of being affected and the importance of following recommended remediation directions in the notification letters, according to the study.

As consumers continue to be inundated with information about data breaches, it will be important...
for risk and compliance professionals to ensure their organisations not only proceed with letters that follow regulations, but also break through the clutter providing concise direction and guidance for customers. Without driving data breach awareness and action, if affected customers do end up experiencing fraudulent activity, the experience has proven time and again to negatively impact a consumer’s relationship with the breached company.

Additionally, the aftermath of a breach can be long-lasting, with 48 percent of consumer respondents of the Ponemon Institute study noting concern that their identity would be at risk for years or forever. With increased concerns comes the expectation that organisations will also provide their customers the guidance and tools to protect them following a breach.

Consumer notification letters, therefore, are an integral piece of a company’s data breach response as this content is often the first inkling consumers have that their information may have been compromised and their identities might be at risk. It is imperative these breach notifications be efficient, effective in driving action – and perhaps most importantly – have a compassionate tone.

A well-written letter will help reduce the risk of fallout and maintain consumer trust following an incident. A few best practices that compliance and risk managers should consider are the following:

*Understand the state laws and regulations.*

Currently, there are 48 data breach notification laws within the United States. While some of the laws have similar aspects, they can vary when it comes to consumer notification timing requirements. Since data can be stored anywhere in the world – and not all customers’ data is located in the same state the customer lives – it’s best to seek outside counsel to understand and navigate the complex regulatory landscape. Regardless of the requirements, data breach notification following an incident should be prioritised as soon as relevant information and guidance is available – a key factor to resolution with customers.

*Communicate clearly and frequently.* Depending on the nature and scope of your company and the breach, it may become a media story. So make sure

“Data breaches are quickly becoming one of the top incidents to have an impact on a company’s reputation.”
to first assess and compile all of the information and reports before communicating to the media and your customers. When approaching the notification letter, it should be written simply explaining what happened, how it happened, and what the affected individual should do next. Twenty-three percent of consumers surveyed in the Ponemon Institute study said the notification letter they received would have been better if it had less legal or technical language. Interestingly, 43 percent also said a sincere and personal apology might help convince them to keep their business with the breached organisation. Notably, another 33 percent indicated they don’t want companies to ‘sugar coat’ the information.

Consider providing credit monitoring and identity protection services. The vast majority of customers agree companies should be obligated to provide some form of compensation to consumers affected by a breach. Sixty-seven percent suggest this be provided in terms of cash, product or service, 63 percent said the company should offer them free identity theft protection, and 58 percent said the company should provide free credit monitoring. In the face of a data breach, providing services like free credit monitoring and identity protection services not only protects customers, but can also help the company rebuild its reputation and consumer confidence. The offer should be spelled out in the notification letter with directions on how the individual can enrol.

Data breaches are quickly becoming one of the top incidents to have an impact on a company’s reputation. One of the first crucial steps in a response that can have a major impact on your reputation is the communication to your affected audience, which includes the initial notification. This action should not be overlooked. By understanding evolving consumer attitudes and expectations following a breach as well as the legal requirements, risk and compliance managers can play a role in ensuring the company is doing the right thing – and doing right by its customers. RC

Michael Bruemmer
Vice President
Experian Data Breach Resolution
T: +1 (949) 294 8886
E: michael.bruemmer@experian.com
MINI-ROUNDTABLE

ANTI-CORRUPTION AND COMPLIANCE IN THE ENERGY SECTOR
PANEL EXPERTS

**John Smart**
Managing Partner
EY
T: +44 (0)20 7951 3401
E: jsmart@uk.ey.com

**Jonathan Middup**
Partner
EY
T: +44 (0)121 535 2104
E: jmiddup@uk.ey.com

**David Lister**
Partner
EY
T: +44 (0)131 777 2308
E: dlister@uk.ey.com

**John Smart** leads the Fraud Investigation and Dispute Services practice in London and specialises in investigating fraud, asset recovery and financial investigations. He also advises global companies on risk management and compliance. Mr Smart has extensive experience in carrying out high profile, public investigations into suspected frauds and other sensitive matters. He has also developed our services in intellectual property and has particular expertise in the pharmaceutical, telecommunications, media, energy and utility industries.

**Jonathan Middup** leads the Anti-Bribery and Corruption team in the UK. Mr Middup has almost 20 years’ forensic experience in fraud and regulatory investigations, fraud detection and anti-fraud measures. He is experienced in delivering high quality global engagements responsive to the requirements of courts, regulators and auditors. Mr Middup is a member of the Fraud Advisory Panel and a Certified Fraud Examiner.

**David Lister** leads the Fraud Investigation and Dispute Services practice in Scotland and heads up the Oil and Gas sector team. He is a Certified Fraud Examiner, and has experience of giving evidence in a range of commercial disputes. Mr Lister has advised a range of energy clients in relation to fraud and corruption. He has assisted both the DTI and SFO undertake investigations. He has particular expertise in cross-border investigations and compliance, and has led teams working in over 30 countries.
RC: Could you provide an overview of anti-corruption enforcement activity in the energy sector? What trends have been prevalent over the last 12-18 months?

Lister: While anti-corruption enforcements have been seen across a variety of industries, the energy sector has experienced more bribery enforcement actions than any other. According to Trace International’s 2013 Global Enforcement Report, approximately 20 percent of all foreign and domestic enforcement actions to date have occurred in this sector, including numerous high profile cases. In the last 18 months, we have seen significant fines being levied on energy companies for bribery and corruption breaches. In 2013 the French oil and gas company Total S.A. had to pay $398.2m to settle its FCPA charges, and the Swiss oil services firm Weatherford $152.8m. Both of these are among the most costly FCPA settlements to date. Energy companies often have complex supply chains, and many recent enforcement actions, particularly in the US, have related to parent companies being held responsible for the behaviour of their agents and intermediaries when performing services on behalf of the parent or local subsidiary. Both the Total and Weatherford cases involved improper payments being made via intermediaries.

RC: Why is the energy sector among those most susceptible to corruption risk? Could you highlight any recent cases of note, and their outcome?

Lister: There have been a number of multi-million dollar settlements in recent years by some of the largest energy companies, however this sector cannot be characterised as more corrupt or susceptible to corruption risk. That said, there are particular characteristics of this sector that increase the risk of bribery and corruption. Given the industry usually operates under a tender process, the incentive to pay bribes is often high – for example, energy contracts are often long term with very large potential rewards, therefore individuals may perceive that the potential reward outweighs the risk of paying a bribe to win this contact. Risks also arise from conducting business in emerging markets. Scarcity of natural resources in more established markets means companies are looking to access new reserves in emerging markets. Unstable political situations and the lack of infrastructure and controls necessary to combat corruption can make these locations inherently risky from a bribery and corruption perspective. Further, this sector involves frequent dealings with government officials either directly or through wholly or partially state-owned companies. For example, obtaining the licences for an oil field – leads to increased interaction
with government officials. Emerging markets tend to be excessively bureaucratic, which results in many touch points with government where bribes can be demanded. Finally, there is a heavy reliance on third parties. Energy companies frequently hire third parties, such as engineering, procurement and construction management (EPCM) businesses, to manage their in country operations. Similarly, companies contract with national oil companies to form a joint venture to develop oil and gas fields. The other JV partner may appoint government officials to sit on the board of directors to protect the interests of the state. These arrangements can increase the risk of perceived or real conflicts of interest and damage the reputation of the company. Additionally, these contractual arrangements can leave integrated oil companies liable for any bribes or kickbacks paid via the other JV party.

**Middup:** The FCPA has been in place since 1977 but we have seen strong enforcement actions taking place only in recent years. The UK Bribery Act 2010 also increased the risk associated with bribery and corruption. The FCPA and UKBA both have international reach and therefore both impact the way global energy companies operate around the world. Compared with other sectors, energy companies are advanced in their understanding of the legislation and also in how to apply it to business practice – an area where many businesses fall down. In particular, we have seen global energy companies carefully considering the third parties that they use in remote locations, given the risk they are exposed to if these third parties engage in paying bribes or corrupt activity. The challenge for the energy companies is implementing global policies

**“While anti-corruption enforcements have been seen across a variety of industries, the energy sector has experienced more bribery enforcement actions than any other.”**

*David Lister, EY*
to address the FCPA and UKBA which are then also tailored to local risk factors.

**RC:** To what extent do you expect the regulatory environment for global energy companies to become more onerous in the years ahead? How will emerging markets factor into this trend?

**Middup:** We expect the regulatory environment will become stricter over time, with the trend for more countries to take this issue seriously, particularly in the emerging markets. For example, recently, countries such as Brazil, China and Russia have either introduced or revised their legislation regarding bribery and corruption. In addition, cross collaboration between regulators will increase the number of overseas investigations and will continue the push for more international regulations. With emerging markets as well as mature ones, it is the appetite for enforcement that determines how strongly the regulatory environment is felt rather than the regulations themselves. The evidence of enforcement is mixed, with the US continuing to take a lead.

**RC:** Given continued investment and exploration in frontier and emerging markets, what steps can firms take to ensure anti-corruption compliance throughout their supply chain, including associated third-parties?

**Smart:** Companies should carry out proportionate due diligence on third parties, using a risk based approach. They should use risk profiling to decide what level of integrity diligence to conduct on a third party. It is important to have a consistent and structured approach – as regulators are likely to scrutinise the consistency of the process and decision making. Having an effective monitoring strategy is critical for energy companies, especially after the implementation of an anti-corruption compliance program. This typically includes in-

“We expect the regulatory environment will become stricter over time, with the trend for more countries to take this issue seriously, particularly in the emerging markets.”

*Jonathan Middup, EY*
country testing. Also important is training the team operating in these markets. This is crucial as these teams can be operating in markets where bribery and corruption are widespread and may be seen as a way of doing business. Changing the mentality through training is critical and we have found that face-to-face training is the most effective. The training should be focused on those individuals operating in the markets most at risk from bribery and corruption.

RC: What key considerations should energy companies make when performing due diligence on potential third-parties? Do they often fall short when it comes to thorough background checks?

Lister: About 70 percent of recent FCPA actions involve third party intermediaries. In recent years, the energy sector has taken significant action to address the risk; integrity diligence is becoming a well-developed and embedded process. Sixty percent of companies in the energy sector have a background checking process for third parties. Organisations need to know that their third parties are acting with integrity and are not exposing the organisation to risk, and that the third party is capable of delivering what it is engaged to deliver. They need to understand the relationships the third party has with any politically exposed persons or sanctioned entities. They need to know that the third party shares their commitment to ethical business practices. There are a number of key considerations to make when performing due diligence. First, it is important to ensure that the entire population of third parties is addressed. An essential first step is, therefore, to fully understand who the third parties are. This will not necessarily be easy – for example, where a company operates from a number of diverse locations and there is no central oversight of contracts entered into by subsidiary locations. Second, due diligence should be performed on all third parties, commensurate to the level of risk. An initial assessment of the risk profile of each third party should be undertaken to inform the level of due diligence that is appropriate. Third, if a

“Companies should carry out proportionate due diligence on third parties, using a risk based approach.”

John Smart,
EY
background check identifies red flags for a particular third party, this does not necessarily mean that the third party cannot be accepted, but a company should first determine whether measures can be put in place to appropriately mitigate any identified risks. Fourth, third party due diligence should not be treated as a one-off exercise. For a program to be effective, third parties should be subject to periodic reassessment and approval. For example, a subsequent change in the beneficial ownership of a third party may change the company’s perception as to whether a relationship with this third party is desirable. Finally, sufficient resources – both financial and personnel – should be allocated to ensure that the third party due diligence program can operate effectively. The costs of implementing such a program should not be underestimated.

**RC: Tone from the top is vital in establishing core values, ethics and principles. How can senior energy executives transform words into action and promote a culture of compliance through the company?**

**Smart:** Monitoring is key to ensuring people are actually adhering to the company’s policies and procedures. If issues are discovered, these need to be taken seriously by senior management and acted on appropriately. If, for example, it becomes common knowledge within the company that people can make facilitation payments to win contracts without any repercussions, this completely undermines the whole anti-bribery and anti-corruption framework within the company. Disciplinary procedures need to be clearly outlined so employees know what is expected of them as well as the consequences if they do not follow the rules. More importantly, tone from the top needs to shift to tone from middle management. A true culture of compliance cannot be fully created until performance is aligned to risk.

**RC:** What additional advice can you offer to energy companies on tackling corruption? Do you foresee any major compliance issues arising in the next 12-18 months?

**Lister:** As business in emerging markets continues to grow for the oil and gas sector, companies will be increasingly challenged by bribery and corruption risks. The current trend of high FCPA penalties in the sector, coupled with the recent introduction of new or updated anti-bribery legislation in many countries across the world, means that energy companies will be subject to continuing and increasing scrutiny. This requires significant management focus to comply with anti-bribery and anti-corruption regulation. Energy companies need to address their corruption risks proactively by implementing an effective anti-corruption compliance program. Although no measure can absolutely guarantee that a company
will eliminate all risk of corruption occurring, it can substantively mitigate these risks through their timely identification and treatment. Additionally, companies may also be in a better position to demonstrate the measures that were taken to manage such risks, should a potential breach be identified and scrutinised by regulatory authorities. We can expect prosecution by the Serious Fraud Office and more focus on individuals as well as companies. Furthermore, as energy companies continue to expand their operations to high-risk jurisdictions, we can expect more attention to be given to third parties and intermediaries. Lastly, big data and the way energy companies govern and protect their information will be another key area of attention. RC
PERSPECTIVES

DON’T BE AN OSTRICH: LIABILITY UNDER THE FCPA FOR IGNORING INDICATIONS OF POSSIBLE BRIBERY

BY LINA A. BRAUDE AND YULIYA KUCHMA
> BAKER & MCKENZIE LLP

When the US Congress enacted the Foreign Corrupt Practices Act (FCPA) in 1977, the public record revealed a debate over what should constitute ‘knowledge’ of an improper payment under the anti-bribery provisions of the FCPA. There was no controversy over ‘actual knowledge’ since it was clear that a company or individual could be culpable if he or she actually knew about a bribe scheme. However, Congress extended this concept to include what is known as ‘constructive’ knowledge. According to the statute, knowledge exists when a person is aware that a “result is substantially certain to occur” or a person has a “firm belief that such circumstance exists”. The term ‘knowing’ includes conscious disregard, deliberate ignorance and willful blindness. Think of the ostrich who intentionally puts its head into the sand to avoid, in this case, learning the true facts.
Setting aside the legal concepts, what this means is that a company, or one of its executives, could face criminal liability under the FCPA if indications of potential bribery, or ‘red flags’, are reasonably evident in a transaction and nothing is done to resolve those red flags. If at some point in the future it is learned that a bribe actually occurred, liability could arise even if no one at the company actually knew a bribe had been paid or intended that any such bribe be paid. Merely failing to address the red flags may allow US authorities to allege that the company or one of its executives has violated the FCPA.

What sorts of red flags could indicate potential bribery? Let’s take as an example your company seeking to acquire a target company that does business globally including in countries viewed as high risk from a corruption standpoint, which is virtually every emerging market. The US authorities believe that merely doing business in a corrupt
country is a red flag. In particular, prosecutors were successful in persuading a US federal judge in the Bourke case that it was appropriate to enter into evidence the fact that Bourke’s conduct took place in Azerbaijan, a country known for corrupt business practices. The court stated that the evidence demonstrated “that Bourke was aware of how pervasive corruption was in Azerbaijan generally”. While the US Department of Justice (DOJ) introduced evidence that Bourke actually knew about the promoter’s bribery of Azeri government officials in connection with the proposed privatisation of the Azeri national oil company, the court also permitted the jury to make a finding of ‘constructive knowledge’. The court determined that “a rational juror could conclude that Bourke deliberately avoided confirming his suspicions that Kozeny [the promoter] and his cohorts may be paying bribes”.

With that background, assume that the target does significant business in a high risk country through a distributor which sells primarily to customers that are government-controlled. Assume further that the distributor is responsible for obtaining key government approvals to sell the target’s products. In a pre-acquisition review, you learn that the target has never done any anti-corruption due diligence on the distributor and, despite having compliance audit rights in its contracts with the distributor, the target has never exercised such rights or conducted any form of compliance review. Before you determine what the company should do, consider the following recent FCPA case resolutions.

Ignoring red flags becomes basis for $384m in criminal fines and disgorgement of profits for Alcoa, based on the actions of a single consultant/distributor

On 9 January 2014, Alcoa World Alumina LLC, a majority-owned US-based subsidiary of Alcoa Inc. (Alcoa) pled guilty to violating the anti-bribery provisions of the FCPA and agreed to pay a criminal fine of $209m and forfeit $14m to settle the DOJ’s charges. Alcoa itself agreed to pay $161m in disgorgement to settle SEC’s civil charges. The charges resulted from alleged corrupt schemes used by Alcoa subsidiaries to funnel money to foreign officials in Bahrain through a consultant/distributor in order to obtain business with a government-controlled aluminum smelter.

This case is notable because it is the first use of criminal FCPA enforcement built on a ‘constructive knowledge theory’, described as ‘conscious disregard’ by one of the executives of red flags evidencing corrupt misconduct.

The language of the plea agreement indicates that the government interpreted the direct delivery of alumina by an Alcoa subsidiary to the Bahraini end users, despite the existence of a distributorship agreement with the consultant, as a red flag. When Alcoa’s executive was asked by the legal department about the purpose of a distribution agreement with the consultant’s entities, he responded that this is “something that Bahrain Government wants and
that Alcoa shouldn’t get too involved with how the Distributor and the Government interact”. Based on the distribution agreement, the consultant had the right to mark up prices on alumina from Alcoa to the end user. The Alcoa subsidiary also sought and received approval to extend credit lines to the consultant’s entities even though the consultant refused to provide such entities’ financial statements to Alcoa’s credit department. Allegedly, the credit lines were “significantly greater than those granted by Alcoa to any other third party”. The government claimed that by doing so Alcoa “enabled the purported distribution scheme”. The government alleged that these red flags should have put Alcoa on notice that the distribution agreement was a sham. However, Alcoa failed to follow up on such red flags and entered into more distribution agreements. Both the SEC and DOJ asserted that Alcoa ‘consciously disregarded’ the fact that the consultant’s role in Alcoa’s supply chain may have been to generate funds to pay bribes to Bahraini officials.

In each instance in which the government alleged that Alcoa’s subsidiary ‘consciously disregarded’ red flags, there was evidence of legitimate commercial and legal arrangements. However, where bribes are paid over an extended period, the government will review the transactional history through the lens of such bribery and will reinterpret events, statements, documents and other evidence in light of that bribery.

Failure to recognise red flags evidencing potential corrupt practices at a subsidiary can be the basis for an FCPA enforcement action.

On 30 December 2013, Archer Daniels Midland Company (ADM) reached a settlement with the DOJ and the SEC of allegations under the FCPA relating to conduct by ACTI Ukraine, ADM’s indirect majority-owned Ukrainian subsidiary, and ACTI Hamburg, ADM’s majority-owned German subsidiary.

According to the case resolution documents, from 2002-2008, ACTI Hamburg and ACTI Ukraine engaged in multiple fraudulent schemes and paid third-party agents to channel bribes to Ukrainian government officials to obtain VAT refunds owed to ACTI Ukraine by the Ukrainian government. According to the documents, ACTI Hamburg and ACTI Ukraine paid roughly $22m to vendors to pass nearly all of that “Failure to recognise red flags evidencing potential corrupt practices at a subsidiary can be the basis for an FCPA enforcement action.”
money to Ukrainian government officials to obtain over $100m in VAT refunds, to which ACTI Ukraine was entitled. The SEC and DOJ alleged that the VAT refunds obtained by ADM’s subsidiaries though improper payments gave ACTI Ukraine a business advantage resulting in a benefit to ACTI Hamburg and ACTI Ukraine of roughly $41m.

The SEC charged ADM with violations of the FCPA books and records and internal control provisions and ordered it to pay $36.5m in disgorgement and prejudgment interest. In a parallel DOJ action, ACTI Ukraine pleaded guilty to one count of conspiracy to violate the FCPA anti-bribery provisions and agreed to pay a criminal fine of $17.8m. In addition, ADM entered into a non-prosecution agreement with the DOJ for what it appears from the language of the agreement was ADM’s knowing failure to implement and maintain adequate controls over the activities of its subsidiaries in connection with the use of third parties.

In contrast to the Alcoa case, there is no doubt that ACTI Hamburg and ACTI Ukraine were aware of the misconduct. But there is no clear evidence that ADM, the parent company, was aware of the conduct of its subsidiary and, in holding ADM directly accountable through a non-prosecution agreement the DOJ appeared to have relied on a constructive knowledge theory. According to the non-prosecution agreement, “an ADM executive in the tax department sent an email to the head of the international tax organization” and stated that in order to recover $100m of the VAT refunds a Ukrainian subsidiary paid 30 percent to local charities. Such ADM executive further informed two other executives in ADM’s tax department that “he had spoken with the head of the international tax organization and that ‘the bottom line is that ACTI is getting screwed by someone...[T]he consensus is that there is no way legislation could require this situation’”. Apparently, in the eyes of the DOJ this evidence is sufficient to compel ADM to enter into a non-prosecution agreement. Although a non-prosecution agreement is a resolution which falls just short of a formal criminal resolution, it imposes three year reporting obligations on ADM and payment of a $9.45m fine.

While it is clear that ADM’s executives were aware of some concerns related to legal procedures for obtaining a VAT refund, the case indicates how aggressively the DOJ will hold accountable companies which fail to recognise and act upon red flags.

Prosecution of Weatherford International for internal controls violations is equivalent to the DOJ pursuing a constructive knowledge theory for bribery.

On 26 November 2013, Weatherford International, a Swiss oil services company that trades its shares on the New York Stock Exchange, and its Bermudian subsidiary, Weatherford Services Limited, reached a settlement with the DOJ and the SEC regarding alleged FCPA violations in Africa, the Middle East and Europe. Alleged bribery of foreign officials enabled Weatherford to obtain a dominant position and earn
proceeds of $54.4m. Weatherford International and its subsidiaries agreed to pay $152m in fines and $65.6m in disgorgement, prejudgment interest and civil penalties.

In this case, the DOJ appeared to use the criminal prosecution of internal controls violations as an alternative to a constructive knowledge theory. The DOJ charged Weatherford International under the accounting provisions of the FCPA for “knowing failure to implement internal accounting controls”. The deferred prosecution agreement, however, does not recite evidence of Weatherford International’s knowledge of corrupt misconduct by its subsidiaries. Instead, in the case of the joint venture established by one of its subsidiaries in Africa, the DOJ states that Weatherford International did not conduct “any meaningful due diligence of either joint venture partner” even though the joint ventures were controlled by foreign officials and their relatives, nor did it investigate why the local entities were partners in the joint venture despite the fact that such local partners “did not contribute capital, expertise, or labor to the joint venture”. It appears that the DOJ interpreted the parent company’s failure to take preventive measures to address the potential red flags in these high risk operations and countries as the evidence of ‘constructive knowledge’.

The DOJ’s position is that Weatherford International created “a permissive and uncontrolled environment,” in which employees of certain of its subsidiaries “were able to engage in various corrupt conduct”. It appears from the deferred prosecution agreement that Weatherford International’s failure to conduct compliance due diligence of third parties and business transactions, to duly investigate allegations of illegal conduct, and to implement its policies at its subsidiaries and newly established joint ventures, is considered a sufficient ground for charging the company with criminal violations of the FCPA’s internal control provisions. In other words, failure to have an effective anti-corruption program can be a criminal violation of the accounting provisions of the FCPA.

Pre-acquisition due diligence and post-acquisition integration as effective safeguards

Going back to evaluating an acquisition of the target operating in a high risk jurisdiction using third parties to interact with government-controlled end-users, what can you do to protect your company from liability? Appropriate due diligence of the target followed by prompt and comprehensive remediation and integration to ensure compliance with the parent company standards, policies, procedures and applicable anti-corruption laws are critical tools to minimise the risk of criminal liability for post-acquisition corrupt activities at the target. A failure to conduct such due diligence, in light of the Bourke case and the three cases described above, could expose your company to criminal and administrative FCPA liability if it comes to light that
the target company has been paying bribes through its distributors in the high risk market.

The DOJ/SEC FCPA Resource Guide to the U.S. Foreign Corrupt Practices Act articulates ‘best practices’ for pre-acquisition due diligence which include: (i) review of the target’s sales and financial data; (ii) review of its customer contracts, and its third party and distributor agreements; (iii) performance of a risk-based analysis of the target’s customer base; (iv) audit of selected transactions engaged in by the target; and (v) discussions with the target’s general counsel, vice president of sales, heads of internal audit and compliance functions about corruption risks, compliance efforts, and any other corruption-related issues that have surfaced at the target over the past.

If any specific red flags are uncovered in the course of due diligence, they must be properly reviewed to ensure there is sufficient understanding of the issues so that they can be resolved on a timely basis.

Conducting pre-acquisition due diligence in line with the best practices articulated by the US enforcement authorities would not only address the risk of liability under the FCPA but it also allow the buyer to discuss with the seller the exposure of the target before the acquisition and request additional contractual protections or price adjustments. The due diligence results would become a starting point for post-acquisition remediation.

The recent enforcement actions demonstrate that even if there is no clear indication of knowledge of possible bribery, failure to implement effective mechanisms that would detect and prevent it may be interpreted by the DOJ as ‘ostrich-like’ behaviour resulting in enormous costs to a company. These cases also reaffirm the importance of being vigilant and maintaining a robust anti-corruption compliance program to avoid the aggressive tactics of the DOJ and the SEC in FCPA enforcement. **RC**

---

**Lina A. Braude**
Partner
Baker & McKenzie LLP
T: +1 (202) 452 7078
E: lina.braude@bakermckenzie.com

---

**Yuliya Kuchma**
Associate
Baker & McKenzie LLP
T: +1 (202) 835 1889
E: yuliya.kuchma@bakermckenzie.com
MINI-ROUNDTABLE

IMPACT OF BRAZIL’S CLEAN COMPANIES ACT
PANEL EXPERTS

Richard Fogarty leads Berkeley Research Group’s (BRG) Investigations and Compliance Practice and is a director. He has over 17 years of investigative and legal experience and is a leader of BRG’s Latin America practice. He has conducted hundreds of investigations across the globe. Mr Fogarty is an expert in matters related to regulatory compliance, complex internal and external fraud, asset searches and investigations, Foreign Corrupt Practices Act (FCPA), anti-money laundering and ant-terrorist financing, investigative due diligence, and supply chain and employee theft.

Richard Fogarty
Director, Latin America Practice Leader
Berkeley Research Group
T: +1 (401) 824 4097
E: rfogarty@brg-expert.com

Thiago Jabor Pinheiro is a senior associate at Mattos Muriel Kestener Advogados (MMK) in São Paulo, Brazil. Mr Pinheiro’s practice focuses on anti-corruption compliance and government relations. Prior to joining MMK, Mr Pinheiro was a Visiting Lawyer at the New York Office of Sullivan & Cromwell LLP. Mr Pinheiro graduated from Universidade de Brasília (2006), and holds Masters Degrees from Universidade de Brasília (2009) and Harvard Law School (LL.M., 2010).

Thiago Jabor Pinheiro
Senior Associate
Mattos Muriel Kestener Advogados
T: +55 11 3149 6220
E: tjabor@mmk.com.br

Isabel Franco is a partner at the Brazilian law firm KLA - Koury Lopes Advogados. Her practice is concentrated predominately on matters of business law, in general assistance to multinational clients in their investments in Brazil, advising especially on mergers & acquisitions, contracts and regulatory matters with a main focus on compliance and anti-corruption legislation including the FCPA, UK Bribery Act, Dodd-Franck Act, OECD Anti-Bribery Convention and the Brazilian Clean Companies Act.

Isabel Franco
Partner
Koury Lopes Advogados
T: +55 11 3799 8189
E: ifranco@klalaw.com.br

Erica Sarubbi is a senior associate in the compliance group of Trench Rossi & Watanabe, a São Paulo law firm that cooperates with Baker & McKenzie.

Erica Sarubbi
Senior Associate
Trench Rossi & Watanabe
T: +55 11 3048 6800
**RC: How would you describe Brazil’s fraud and corruption environment?**

**Fogarty:** We see an increased level of concern from both multinational entities and Brazilian companies, not only about existing regulations such as the FCPA and the UK Bribery Act, but also with Brazil’s Clean Companies Act. What remains to be seen is how well enforced the Act is in reality. Infrastructure projects and concession contracts around both the World Cup in 2014 and the Olympics in 2016 will undoubtedly create situations where the Act can be applied and where both corruption and fraud will occur. What happens over the next three years and what action is or isn’t taken by regulators during that time against companies engaging in corrupt activities in Brazil, will define the strength of the Clean Companies Act. I would also add that the ‘atmosphere’ for change in how endemic problems like corruption are viewed in Brazil is changing. Recent protests over the last year show an increasing level of frustration by the populace with fraud and corruption and the perception that regulators and politicians have looked the other way for too long.

**Franco:** Unfortunately Brazil is a very corrupt country as can be seen by the Transparency International CPI of 4.2 which puts us in the 72nd position worldwide in 2013. Our anti-corruption team’s experience attests to this fact by our participation in M&A projects, due diligences and internal investigations in past years, not to mention recent scandals revealed by the media involving higher ranking members of the country’s administration and state controlled companies such as Petrobrás. Also, investigations conducted by tax, labour and police inspectors to companies are usually accompanied by a request for a bribe by the public agent involved in the case. Lastly, there are also numerous cases related to overpriced public contracts. The 2014 World Cup here in Brazil has enhanced the corruption scenario with infrastructure constructions and work that in many cases was promised but has not even taken place.

**Pinheiro:** Over the past few years, Brazilian authorities have been making progress in their fight against fraud and corruption. The most telling example is the recently concluded Mensalão case, a corruption scheme uncovered during the first Lula administration, in 2005. A number of high-profile politicians, such as Lula’s first Chief of Staff, were involved in the scheme, and there was a widespread feeling among the population that such politicians would never serve time in jail. However, they were prosecuted and convicted by the Federal Supreme Court in 2013, and are now incarcerated. Additionally, Brazilian authorities have been implementing new measures to increase government transparency and prevent corruption. The latest development in this
Area was the enactment of Brazil’s Clean Companies Act, an innovative legal instrument that makes companies strictly liable for acts of corruption and bid rigging practiced by their employees and agents.

Sarubbi: Corruption is still a serious concern in Brazil, with the country ranking 72nd on the Transparency International Index. There has been a great effort to change this situation, and Brazil recently enacted new laws to curb fraud and corrupt practices, such as a new Money Laundering Law, a Conflict of Interest Law and most recently the anti-corruption law, known as the Clean Companies Act, which sets forth strict liability for companies, both domestic and foreign, that commit acts of corruption and acts against the public administration. Although corruption already constituted a crime, under the Brazilian Criminal Code only individuals were criminally liable for corrupt practices. The new anticorruption law broadens the scope and creates the direct liability – civil and administrative – for legal entities doing business in Brazil. The enactment of the new law occurs at a time in which Brazilian citizens have been protesting against corrupt practices and should help in the process of developing a greater corporate culture of ethics and compliance as well as a more level playing field for multinationals that were already subject to other severe anticorruption laws, when conducting business in Brazil.

RC: What were the key drivers that led to the introduction of the Clean Companies Act?

Franco: I am a firm believer that the Act only passed because of the pressure that the Organization for Economic Cooperation and Development (OECD) put on Brazil to finally enact the law. After all, this was a commitment Brazil made back in 2000 under President Fernando Henrique’s administration. After the Labor Party took office in Brazil in 2003 the bill was forgotten in Congress. Brazil was one of the only countries that had ratified the OECD Anti-Corruption Convention which had not enacted a Clean Companies Act. After the enactment by the UK of the Bribery Act, Brazil lost its excuse that even developed countries had not passed a similar statute. As the ‘B’ of the BRIC group, the fact that it was the only country without an anti-bribery act relating to legal entities was more than embarrassing: it directly jeopardised the country’s investment rating, which was downgraded by one of the international credit-rating agencies. The second driver was that Brazil had a massive wave of protests in June 2013 and one of the main targets of the population was corruption in the government. One of the attempts to respond to people’s claims was the sudden enactment of the Act on 1 August by President Dilma Roussef. She was determined to silence the crowds with one demonstration that the
government could fight corruption. The Act was a good idea.

**Sarubbi:** One of the key drivers for adopting a very strict anticorruption law is the fact that Brazil is a signatory of the OECD Convention on Combating Bribery and therefore has to abide by its strict requirements to combat bribery of foreign public officials in international business transactions. In 2007, Brazil was evaluated as part of the OECD’s Phase II review of Brazil’s implementation of requirements of the OECD Convention. As a result of the review, the OECD recommended that Brazil should “take urgent steps to establish the direct liability of legal persons for the bribery of a foreign public official”. The new legislation fulfills this requirement. Additionally, the increased importance of Brazil in the world’s economy also plays a great part in the enactment of the new law, as companies are wary of investing in a country with a high corruption risk.

**Pinheiro:** The Clean Companies Act was the result of long-term and short-term drivers. The most important long-term drivers were the international anti-corruption treaties signed by Brazil during the 1990s, particularly the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. Such treaties required Brazil to criminalise the bribery of foreign public officials and to implement related measures. This process began in the early 2000s, but unfolded slowly. The draft bill, which eventually became the Clean Companies Act, was submitted by the Federal Executive Branch to Congress in 2010. Then, in June 2013, a wave of demonstrations erupted in Brazil to protest against the bad quality of public services and corruption. Among other measures to answer the cry of the streets, the government asked Congress to give absolute priority to the approval of the Clean Companies Act, a request that accelerated the legislative process of the bill and led to its introduction as law in August 2013.

**RC: What operational and compliance challenges do the Act’s key provisions create for Brazilian companies, as well as foreign companies doing business in Brazil?**

**Pinheiro:** Brazilian and foreign companies that already have sophisticated compliance mechanisms in place to comply with similar rules, such as the FCPA and the UK Bribery Act, should have no difficulty adapting to the Clean Companies Act. Medium-sized and smaller companies, however, will probably face a number of challenges in the coming months. The main operational challenge is implementing adequate internal compliance programs. Putting in place an appropriate structure requires a financial investment that not all companies are willing, or able, to make at this point.
Also, there is a lack of qualified professionals to manage such programs, which drives up their cost. The main compliance challenge is to foster a new business culture, one in which the workforce sees itself as the first line of defence against corruption. I am confident that both challenges will be eventually met, though.

**Fogarty:** In particular we have seen an uptick in companies in Brazil, as well as foreign companies, conducting various levels of due diligence on their party providers, whether they be distributors, salespeople or other vendors. I suspect that with the enactment of the Clean Companies Act, Brazilian companies in particular will need to pay greater attention to the strict liability provisions of the Act. In our experience, Brazilian companies have not been focused on the activities of third parties who represent their company and only recently has there been a trend toward conducting the due diligence that multinational companies have been doing upon entering the Brazilian market. Traditionally, due diligence has been viewed as discretionary and costly. That will change as companies begin to recognise that the cost of upfront due diligence pales in comparison to the potential for significant fines and costs associated with reputational damage under the FCPA and now Brazilian law. There will also be a period of adjustment as companies which have not dedicated sufficient effort to beefing up their compliance staff and resources undergo a difficult corporate culture change. Specifically, companies will need to ensure that management and employees are trained and understand the importance and value of conducting business in a way that is compliant with the Clean Companies Act – a not insignificant endeavour.

**Sarubbi:** The new anticorruption law is a pioneer in setting forth strict liability for companies for acts of corruption and other acts against the public administration. The law is applicable to all business organisations in Brazil, whether incorporated or not, as well as any foundation or association, and to all foreign companies with a presence in Brazil. Although companies that were already subject to other anti-corruption laws, such as the FCPA or the
UK Bribery Act, may already be prepared for some of its provisions, certain revisions to internal policies and procedures, as well as training, will likely have to be considered in view of the broader scope of the new law. Additionally, Brazilian companies that do not have adequate compliance programs to prevent illegal conduct will have to undergo a significant change. Another challenge, as already established by other important anticorruption legislations, is that companies may be liable for acts committed on their behalf or for their interest by any third parties, which increases exposure as many companies use third parties to cover the vast territory of Brazil. In order to be compliant with the Clean Companies Act, companies will need to dedicate more resources to areas of risk, such as conducting comprehensive due diligence and background checks on partners and any third parties acting on their behalf, periodically training their employees on anti-corruption and public tender regulations, and implementing adequate programs to monitor compliance. Such changes require investment of time, money and, in some cases, will require a significant cultural change and commitment from senior management to be effective.

Franco: To date, and not surprisingly, the government has not yet enacted the long awaited guidelines for the Act, which, in accordance with Brazilian norms, have to be promulgated in the form of law. We believe this delay is due to pressure placed on the government by companies that do not want to bear the costs of a compliance program. In fact, the Clean Companies Act signals that the existence of mechanisms and internal compliance procedures, effective codes of ethics, due diligence, and incentives for whistleblowers, will be considered by the authorities when sanctioning a company that has violated the Clean Companies Act. Considering that monetary fines may vary from 0.1 to 20 percent of the company’s gross revenues in the fiscal year prior to the initiation of the enforcement procedures, the existence of a robust compliance program may lead to a significant reduction in any penalty to be paid if a company has infringed the Clean Companies Act.

RC: What penalties can companies expect to face in the event that prohibited activities are investigated and prosecuted by the Brazilian authorities?

Sarubbi: The Clean Companies Act sets forth severe judicial and administrative penalties for companies that violate the law. Penalties can be monetary, such a fine in the amount of 0.1 to 20 percent of the gross revenue of the company of the previous year, or, if this criteria cannot be used, an amount between R$6000 and R$60m. Non-monetary penalties include prohibition to receive incentives and public financing from one to five years, partial suspension or interdiction of its activities and
even the compulsory dissolution of the legal entity. Considering the seriousness of the offences, it is likely that the new law will be severely enforced by authorities. With that, it is possible that there will be an increase in the prosecution of individuals, based on evidence obtained in such enforcement actions.

**Franco:** Initially, we should emphasise that the Act establishes strict liability for the offending entity. Once the offence is determined, the offending entity will be subject to sanction even if it has not obtained any benefit from its wrongdoing under the law, or its employees or agents act on its behalf without authorisation, or a third party, whether a natural person or a legal entity, is used for the wrongdoing. The judicial sanctions encompass, in addition to full disgorgement of the benefits illegally obtained, forfeiture of assets, rights or other values obtained as a result of the wrongdoing; partial suspension or interdiction of corporate activities; compulsory dissolution; and debarment, which includes the prohibition from receiving incentives, subsidies, grants, donations or loans from public financial institutions for one to five years.
**Pinheiro:** Companies may face administrative penalties and civil prosecution as a result of prohibited activities. The administrative penalties available are fines and the widespread announcement of any penalties imposed, in a widely read newspaper and in the company’s website, for instance. Besides the administrative procedure, authorities can file a civil lawsuit against the company, seeking to impose the following additional penalties: disgorgement of unduly obtained funds or assets, suspension of activities, prohibition to receive public incentives, subsidies, donations or loans for a period of 1-5 years, and, in certain specially grave circumstances, the dissolution of the company.

**RC: Have there been any criticisms or perceived shortcomings of the new Act? If so, how are these likely to be addressed?**

**Franco:** Although the Act holds promise in its efforts to change Brazilian culture, scholars and practitioners in the area are concerned about certain aspects of the new law. One issue is what competent authority will apply the Act, since it will need to establish and conduct administrative proceedings and enter into leniency agreements provided by the Act. In other words, the Act neglected to designate a specific single government authority to establish and conduct administrative proceedings. This designation would have allowed the agency to become a qualified body, to develop the relevant technical expertise and to make consistent and equal decisions. Rather than establish a specialised agency, the Act allows any of the highest authority of the executive, legislative and judicial arms of each county, state and union to be a competent authority. Therefore, jurisdiction to enforce the Act is diffuse, which will lead to inconsistency and no standard application of the law, not to mention that it may empower the very authorities that could be involved in cases of corruption to apply related sanctions. To illustrate, Brazil has more than 5500 municipalities. In principle, any of these municipalities’ mayors may apply the law. Unfortunately, we know that mayors themselves are the most likely government official to request and take bribes. In this situation, a mayor will not then start procedures against a company upon receipt of a bribe. Allowing them to assume such a role is like putting foxes in charge of a henhouse.

**Pinheiro:** Some provisions of the Clean Companies Act have generated a lot of debate and criticism. Three issues however, are generally perceived to be among the most troublesome. The first is the pulverized enforcement power granted to authorities. The Act allows any public entity in any sphere – federal, state and municipal – or branch of government – executive, legislative and judiciary – to initiate enforcement actions. Companies fear that not all public entities will have the technical expertise required to promote a consistent and
uniform application of the Act, leading to conflicting decisions and a lot of uncertainty. The second issue relates to leniency agreements, which have a relatively limited scope of protection and may need to be negotiated with multiple entities at once. A third issue is the joint and several liability of parent companies, subsidiaries, affiliates and JV partners – under the scope of the JV agreement – for any fines imposed on the company, which may end up affecting entities that have no influence over a company’s actions. Further regulation of the Act by a Decree, which has not been issued as of June 2014, may clarify some of these issues. However, as there is no expectation that the Act itself will be amended anytime soon, these issues are likely to be addressed by the day to day application of the Act by authorities and the courts.

Sarubbi: One of the main concerns regarding the Act is the lack of a centralised enforcement authority. The Act sets forth that the Office of the Federal Comptroller General (CGU) has authority to investigate, prosecute and sanction illegal acts committed against the foreign public administration. Regarding the administrative sanctions, for acts against the national public administration, the authority responsible for the initiation and judgment of the proceeding is the highest authority of the relevant agency or entity of the executive, judiciary and legislative powers. The CGU will also have concurrent authority to initiate administrative proceedings against legal entities and to audit proceedings handled by other authorities.

RC: Given the short timeline between the introduction of the Act and its implementation, do you believe companies are sufficiently prepared for its strict legal framework, and ready to adapt?

Fogarty: There was and is an element of ‘wait and see’ among companies in Brazil. In other words, some companies are hedging their bets with the Clean Companies Act, not taking appropriate internal efforts to identify risks and adopt controls that come into compliance with the new laws, not just previous ones. Until the first shoe drops, and the first company or individual is prosecuted, many companies incorrectly may defer serious efforts to comply. That is a mistake. The Clean Companies Act will take into account when applying penalties such mitigating factors as an effective compliance program and controls, cooperation, and so on. That requires a proactive approach, not a ‘wait and see’ one.

Sarubbi: The new law was pending legislative approval for a few years and several companies were already subject to severe anticorruption laws. However, some companies were not prepared for the enactment of the new law. Therefore, it
is important that such companies assess their risk areas and immediately act to prevent illegal conduct. Companies should conduct comprehensive risk assessments and use that as a starting point to create or enhance compliance programs. The Clean Companies Act establishes that some factors can be considered by the authorities when applying penalties to legal entities, such as the cooperation of the company in investigations, and the existence of an effective compliance program. Additionally, there is also the possibility of entering into leniency agreements with the public administration, in some circumstances. All those factors clearly indicate that companies should now have sufficient controls in place to prevent, monitor and immediately remediate improper conduct.

Pinheiro: The period of six months between the enactment of the Act and its date of effectiveness did receive some criticism at first, but many companies were able to make considerable progress within that timeframe. The main problem, however, is that the Decree required to further regulate the Act was not issued during that transition period, and as of June 2014 remains under review by the Office of the Chief of Staff. Therefore, there is still some uncertainty about key aspects of the Act, and many companies are reluctant to commit their resources to implementing internal mechanisms without knowing exactly what the government expects from a good compliance program. We have been advising companies against this passive approach, though, because the Act is in force and may be applied by authorities at any time. The Decree will hopefully be enacted soon, and will provide the missing piece to ensure full commitment by the entire business community.

Franco: Companies are not prepared at all. Our team has been working 24/7 for Brazilian companies and subsidiaries of multinational companies looking to customise their programs in light of the new Brazilian Act. We receive numerous consultations about the meaning of certain provisions or how to deal with certain situations. We are also invited to speak with the board of directors to explain the

“Companies should conduct comprehensive risk assessments and use that as a starting point to create or enhance compliance programs.”

Erica Sarubbi, Trench Rossi & Watanabe
need for compliance the program and the apparent abrupt change in the ‘rules of the game’. In addition, our clients are learning that it is essential to improve their third party due diligence procedures. To top it all, there is a shortage of specialised personnel in the country that can work in-house with companies in this area of compliance.

RC: The Clean Companies Act also holds companies liable for acts of bribery and corruption committed overseas. What adjustments are multinational firms, already subject to the FCPA or the UK Bribery Act, required to make to comply with the provisions of the Brazilian law?

Pinheiro: Multinational companies that already have well-structured compliance programs, such as those subject to the FCPA and the UK Bribery Act, are unlikely to face difficulties. But they need to be mindful of the minor particularities of the Act. The liability for acts committed overseas, for example, only applies to companies incorporated in Brazil. Therefore, multinationals need to comply with the Act in the course of their international operations carried out through a Brazilian subsidiary, especially if the Brazilian subsidiary has foreign subsidiaries of its own.

Another example is that the Act does not allow facilitation payments, which are lawful under the FCPA. A third example is that the Act applies to private bribery, as the UK Bribery Act does, but with a narrower scope: a private bribe only violates the Act to the extent that it affects a public contract or a public tender.

Franco: There should be certain adjustments in, for example, the area of facilitation payments, which are not permitted by Brazilian law in any way. Another provision of the Act, which has already raised eyebrows, is that certain conduct may considered a violation of the Act, such as hindering an investigation or audit by public agencies, entities or agents, or interfering with their work, within the scope of the regulatory agencies and supervisory

“The Act contains several provisions relating to bidding procedures, which are not found in the FCPA and the UK Bribery Act.”

Isabel Franco, Koury Lopes Advogados
bodies of the national financial system. No one knows what this unclear provision encompasses and how it will impact ordinary inspections by government authorities. Furthermore, the Act contains several provisions relating to bidding procedures, which are not found in the FCPA and the UK Bribery Act, that must certainly be taken into consideration by a compliance program. Such acts include defrauding the competitive nature of a public bidding procedure; preventing, hindering or defrauding the performance of any act of a public bidding procedure; diverting or trying to divert a bidder by fraudulent means or by the offering of any type of advantage; defrauding a public bid or its resulting contract; deceitfully forming an entity to participate in a public bid or contract; illegally benefiting from changes or extensions of government contracts; and defrauding the financial/economic balance of government contracts.

**Sarubbi:** Multinational firms that are already subject to the FCPA or the UK Bribery Act usually already have in place robust compliance programs that cover acts of corruption committed internationally. However, the Clean Companies Act not only legislates on corruption acts but it also prohibits acts committed against the public administration, mainly related to acts of fraud or those seeking to thwart the competitiveness of public tenders, regardless of whether or not those acts are linked to corruption. For that reason, even companies that already had a strong a compliance program in place should review their existing policies and procedures in light of the new law, in order to create and disseminate clear policies on what employees and third parties can or cannot do while participating in public tenders.

**Fogarty:** As the Brazilian economy has become one of the largest in the world, despite recent issues, we have seen the commensurate entry of Brazilian companies into the international markets. A number of such companies traditionally had no desire or need to move beyond their own large domestic market. That has changed. In light of the Clean Companies Act holding companies liable for acts of bribery and corruption committed overseas, Brazilian companies should pay close to attention to how their employees and third party representatives conduct business in foreign jurisdictions. Furthermore, with the implementation of the Clean Companies Act now putting Brazilian regulators at the forefront of anti-bribery and anti-corruption efforts in Brazil, one should expect to see an increase in cooperation and sharing of information between regulators and law enforcement in the US, the UK, Brazil and elsewhere. Companies need to keep in mind the recent developments as they look to ensure that their overseas employees and third parties are conducting business appropriately and are part of a compliance program that provides education, training, a due diligence program that
identifies risks associated with both employees and third parties, as well as a mechanism that clearly lays out how reporting and investigation of potential bribery, corruption and fraud are to be handled.

**RC:** One criticism of the new Act is its lack of a centralised enforcement authority. In your opinion, to what extent could this lead to inconsistent rulings and standards?

**Sarubbi:** A number of authorities at federal, state and municipal level can investigate allegations of misconduct and sanction corporations. Among other problems, an initial concern was the lack of specialised enforcement authorities and potential inconsistent outcomes which could cause companies to face uncertainty and lack of precedents over a certain matter. However, the CGU has been involved with the Act since its conception and has the authority to audit enforcement proceedings at the federal level, which could mitigate some of the aforementioned risks. On the State and municipal levels, some states and municipalities have already issued their own regulations and granted authority to enforce the law to specific agencies, such as the State of São Paulo and the city of São Paulo. The involvement of specialised and qualified authorities, at least in the most important states and municipalities, will also be an important factor to mitigate the negative consequences of the decentralised system.

**Franco:** The lack of a centralised enforcement authority is, in my opinion, the most dangerous aspect of this law. Authorities that may be in charge of enforcing the law may be the very ones that consistently request and receive bribes. In any case, even if they were honest and sincerely wished to initiate procedures to investigate an illicit act in their jurisdiction, we doubt that they would have the expertise, sophistication and tools necessary to deal with these cases. Their actions may be disastrous and jeopardise the real investigation and procedures that may make the difference. To illustrate, this week Switzerland has suspended all judicial cooperation with Brazil due to a leak of confidential information involving the investigation of a council member of the Brazilian Audit Court in the Alstom case. As a result, this suspension will freeze at least 10 other cases which were being jointly investigated by Brazil and Switzerland.

**Pinheiro:** The risk exists and it has been a matter of grave concern to the business community and authorities alike. Even the CGU, the agency in charge of anti-corruption policy at the Federal level, has acknowledged on numerous occasions...
that inconsistent rulings and the political use of enforcement power would undermine the full implementation of the Act. But CGU officials have also expressed confidence that local authorities will seek uniform standards under the guidance of the federal government when applying the law, and that courts will be able to resolve any abuse. Only time will tell whether or not these predictions will come to fruition.

**RC: What steps would you advise Brazilian and foreign firms to take to ensure compliance with the Clean Companies Act?**

**Fogarty:** Two things are crucial. One is a strong compliance program and message from management at the top to all employees and third parties. That includes employee and third party training and education. Secondly, as part of that program, companies must implement, and most importantly maintain, an ongoing due diligence of all business partners and third parties. We have seen too many situations where a client conducts initial due diligence on a third party as a ‘one-off’ type of situation, identifies no significant issue and hires or contracts that third party. Then, because there is no ongoing due diligence process in place, problems that arise with the same party – for example, ownership change leading to questionable business practices for example – are not identified in a timely fashion, leading to increased risk of fraud and corruption and costly remediation.

**Pinheiro:** I would advise companies not yet adapted to the provisions of the Act to conduct a careful risk assessment of their sectors to identify and understand the vulnerabilities to which they are subject. Furthermore, they should ensure that their managers understand such risks and are committed to implementing adequate compliance measures to protect the company. Finally, they should seek the assistance of specialised professionals, both internal

“I would advise companies not yet adapted to the provisions of the Act to conduct a careful risk assessment of their sectors to identify and understand the vulnerabilities to which they are subject.”

Thiago Jabor Pinheiro,
Mattos Muriel Kestener Advogados
and external, to carry out the required adaptations as soon as possible, and to make sure any procedures and mechanisms are kept up to date.

**Franco:** Initially, it is fundamental that companies understand the provisions of the Act and how it will apply to them. This exercise includes understanding how the Brazilian system works – the Public Ministry, the police and all of the other authorities that may be involved. Then, with that in mind, companies should raise their internal awareness of how a robust Brazilian compliance program could be effective and beneficial to business in general. Communication of the awareness and the program is essential through live training. This new concept of compliance is practically unknown to Brazilians and Brazilian entities. The introduction of this new world must be explained personally to all who will be exposed to the Brazilian Clean Companies Act.

**Sarubbi:** Companies should be working on creating a strong compliance program that not only covers corruption matters but that also covers public procurement regulations, in order to prevent illegal activities, such as bid rigging or fraud in public tenders. Companies should create and maintain procedures to prevent, detect and remediate prohibited acts, taking into account their main areas of risk. Additionally, it is very important that companies disseminate the content of policies and educate employees on the content of applicable anti-corruption legislation. We recommend that companies conduct regular training sessions for their employees and third parties. Companies should adopt strict protocols to review third parties and business partners and consider creating investigation protocols to effectively investigate allegations of improper conduct. A quick reaction to allegations of wrongdoing can assist companies in stopping further illegal acts. By having complete information regarding a potential issue, companies can also make timely decisions regarding disclosure to authorities and potentially benefit from a leniency agreement and for cooperating with authorities, which is a factor to be taken into consideration for the application of penalties according to the new anticorruption law. Finally, companies will also have to timely consider cooperation with international authorities, considering the increased cooperation among enforcement agencies. **RC**
ONE-ON-ONE INTERVIEW

FRAUD INVESTIGATIONS BY MULTILATERAL DEVELOPMENT BANKS

Lee Marler
Barrister
Bretton Woods Law
T: +44 (0)20 3009 3188
E: leemarler@brettonwoodslaw.com

Lee Marler is a barrister and Joint Head of Chambers at Bretton Woods Law and is a former Director of Operations at the World Bank Integrity Vice-Presidency. He has appeared before the Sanctions Board and has brokered Negotiated Resolution Agreements with the World Bank, immunity arrangements with the Asian Development Bank and is counsel to the African Development Bank’s Integrity and Anti-Corruption Department.
RC: Could you provide a brief overview of multilateral development bank (MDB)-financing? What trends and developments have you seen in recent years?

Marler: The MDBs, namely, the World Bank, the African Development Bank, the Asian Development Bank, the European Bank for Reconstruction and Development and the Inter-American Development Bank, provide billions of dollars each year in loans and donor funding to less-developed countries. International development companies worldwide, which provide numerous and diverse services, are able to compete for and bid on MDB-funded projects. Once the contract is awarded, the winning bidder is responsible for fulfilling the obligations under the MDB financed contract, which can range from IT systems in hospitals to agriculture projects and online tax systems for a developing country’s revenue department. But with this funding comes responsibility, and the MDB community is increasingly seeking to use its influence in the global anti-corruption fight. As such, companies that benefit from MDB funding effectively submit to their investigative jurisdiction and their ability to sanction for misconduct, such as corruption, fraud, collusion and coercion.

RC: To what extent have MDBs developed as major players in the international anti-corruption landscape? How has their role changed over the past 20 years?

Marler: Over the past 20 years, the MDBs have become major players on the international anti-corruption landscape. The power of debarment that these banks wield over contracting parties is such that they must be thought of as distinct jurisdictions in and of themselves. Indeed, the MDBs now run substantial and sophisticated anti-corruption departments that are charged with the responsibility for investigating and punishing allegations of corruption, fraud, coercion and collusion – the sanctionable practices – on bank-financed contracts. Yet these investigative departments – such as the Integrity Vice-Presidency of the World Bank – should not be viewed in isolation, for not only do they interact with each other, they also engage with the law enforcement agencies of their member states and regularly make criminal referrals in respect of matters that they have investigated. Indeed, this is a trend that can be seen with the African Development Bank, which, like the World Bank, now has an established and effective Integrity and Anti-Corruption Department (IACD) that works closely with such agencies as the United States’ SEC.

RC: What key features distinguish MDBs as a source of enforcement from more
traditional enforcement mechanisms, such as the FCPA and UK Bribery Act? What mechanisms and strategies do MDBs tend to employ?

Marler: Perhaps the most significant difference between the anti-corruption departments of the multilateral development banks and the more traditional enforcement mechanisms is the sheer breadth of conduct that might constitute a sanctionable practice; linked to that is the considerably lower threshold for a finding of wrongdoing. Unlike many national bodies which look to criminal statutes and codes for definitions of offences, the MDBs themselves specify what constitutes a sanctionable practice. Almost without exception, companies that work on MDB-financed contracts completely underestimate the scope of the sanctionable practices and how strictly they are enforced. For example, most people think they understand what fraud is; yet few realise that a misrepresentation as to qualifications on a consultant’s curriculum vitae, submitted as part of a bid, could be sufficient to render the entire company debarred from bidding on bank-financed contracts. What is more, not only is mens rea or ‘intention’ not required – since the banks take the view that this fraud can be committed recklessly – their standard of proof is substantially lower: there is no search for evidence to satisfy the decision-maker ‘beyond reasonable doubt’, but rather, the balance of probabilities will suffice. For the banks, the question is: is it more likely than not that a sanctionable practice has been committed?

RC: What are the potential risks and penalties for firms found guilty of fraudulent and corrupt practices while engaged in MDB-financed projects? What sanctions can MDBs impose?

Marler: To be blunt, the consequences for firms found guilty of sanctionable practices can be catastrophic and for a firm which relies on MDB-financed contracts, debarment by one MDB and cross-debarment by the others can spell the end of the company. The sanctions which may be imposed singly or in combination include, but are not limited to: debarment for a specified minimum period; debarment with conditional release or reinstatement; indefinite debarment; conditional non-debarment; letter of reprimand; and restitution or financial remedy. However, the stigma and reputational risk of debarment should not be underestimated, nor should the mischief that competitors can make out of such a sanction, to companies’ detriment. The periods of debarments handed down by the banks can run into years and it is likely that a company will then find its work in other areas under close scrutiny. Companies debarred and cross-debarred by the MDBs often see national aid agencies, such
as DFID or USAID, walking away from them and refusing to allow them to benefit from projects they are financing.

**RC:** To what extent are MDB practices harmonised internationally? How does this heighten the risk of misconduct?

**Marler:** There has been a significant harmonisation in recent years of the practices of the anti-corruption departments of the MDBs, first by virtue of the adoption of unified guidelines for the investigation of fraud and corruption and, secondly, through the signing of the Agreement on Mutual Enforcement of Debarment Decisions, which set out the principle of cross-debarment, whereby the MDB community agrees to mutually enforce debarment actions of the other banks. Moreover, the MDBs have harmonised how they hold corporate structures culpable for sanctionable practices committed by, for example, subsidiaries. Recent years have seen the MDBs become much more litigious in protecting the funds they disburse and there has been a significant increase in the levels of cooperation between them. Intelligence sharing is prolific. The consequence is that the prospect of sanctions proceedings by the MDBs should not be underestimated by companies that undertake work on contracts funded by these lending organisations, for the consequences can be catastrophic.

**RC:** How has cross-debarment affected the behaviour of companies alleged to have engaged in corrupt practices?

**Marler:** Cross-debarment is automatically triggered when a company is debarred by one of the MDBs for a period in excess of a year: the effect is that all of the other MDBs also debar the company concerned in accordance with the decisions of the sanctioning bank. The advent of cross-debarment has upped the stakes considerably for companies that are alleged to have engaged in corrupt practices, since it can, quite literally, spell the end of the company or at very least radically change

*"Just because the accusations are coming from an MDB does not mean that it is not significant or that it will just go away: the burden of proof within the MDB community is low and their reach considerable."*

---

Lee Marler, Bretton Woods Law
the way it operates. Companies must therefore be mindful that their conduct in respect of one MDB may impact on their ability to undertake work for another.

**RC: What is the significance of the settlement mechanisms recently added to the MDB sanction process? What implications does this have for the way investigations will be resolved going forward?**

**Marler:** The settlement mechanisms or ‘Negotiated Resolution Agreements’ (NRAs) within the MDB anti-corruption regime provide companies with the ability to minimise the commercial impact of findings of guilt in respect of sanctionable practices, whilst also offering them a constructive way to reform so as to prevent repetition of the misconduct in the future. NRAs equate, in effect, to prosecution agreements under which a company cooperates for a reduced sanction. Settlement can quite literally be fundamental to the survival of a company, but the terms can be onerous and it is vital in negotiating such a settlement to use specialist counsel and those with experience in the performance of companies’ obligations under such agreements, for non-compliance can render any agreement null and void. NRAs are likely to involve a review of the company’s books and records by an independent team of investigators, who will inspect the company for further evidence of wrongdoing. The company may benefit from immunity in respect of these, whilst the bank may benefit from essential intelligence.

**RC: What advice can you offer to firms facing accusations of fraud and corrupt practices related to MDB financing, or of using fraudulent means to obtain MDB financing?**

**Marler:** Just because the accusations are coming from an MDB does not mean that it is not significant or that it will just go away: the burden of proof within the MDB community is low and their reach considerable. Early action is the key to influencing the course of events and is much more likely to lead to settlement. The MDBs’ sanctions regimes are particularly esoteric and complex, so do not expect the lawyer who does your day-to-day business to be able to competently navigate the process: it is an area that requires the guidance of specialist counsel. Defending a company accused by the MDBs of engaging in sanctionable practices on MDB-financed contracts is not the same as representing a company charged by the SFO of DOJ. Different rules and considerations apply. Experience suggests that a failure to instruct experts all too often has the effect of doing more harm than good, so that when specialist are instructed further down the line, their effectiveness is hindered. **RC**
Mitigating the Risk of Mounting Conflict Mineral Sourcing Regulations

By Kirsten Wallerstedt
> 3E Company

The US and EU conflict minerals and responsible sourcing laws can put a corporation’s reputation at risk – but they may also create opportunities for a business to open new markets. While some companies have struggled to meet even the basic demands of the US law, others that have met the requirements achieve an advantage – suppliers that can give evidence of compliance with these regulations may solidify contracts and secure new business partners more easily than those that fall behind in their ability to procure information from their supplier networks.

What exactly are conflict minerals?

As defined in the US Dodd Frank Wall Street Reform and Consumer Protection Act of 2010, ‘conflict minerals’ are the minerals from which tin, tantalum, tungsten or gold are extracted or obtained as a by-product and directly or indirectly fund or benefit armed groups in the Democratic Republic of the Congo (DRC) region of Africa. These minerals are essential to the manufacture of products such as consumer electronics, cars, clothing, aerospace equipment, medical devices and jewellery. US law requires that public companies discover and publicly report on the presence and source of these minerals.
when present in the company’s manufactured products.

New guidance from the US Securities and Exchange Commission (SEC) on the US law, issued on 29 April 2014, highlighted the dynamic nature of regulations that can affect a business’s supply chain. The changes also underscored the importance of having a supplier engagement system that is flexible and adaptable to meet evolving obligations and demands. The two major conflict minerals initiatives – in the US and the EU – create obligations and opportunities for enhanced risk management, reputation protection and a bolstered bottom line.

Evolving US conflict minerals obligations

This year, the US conflict minerals law survived a major court challenge mostly intact. The US Court of Appeals overturned one aspect of the SEC’s Final Rule on Section 1502 of the Dodd Frank Act. The court declared it a violation of free speech to compel companies to describe their own products as ‘not’ found to be ‘DRC conflict free’.

In response, the SEC issued a statement saying that in the disclosure due on 2 June 2014, companies were no longer required to describe their products as ‘not’ found to be ‘DRC conflict free’, nor as ‘DRC conflict undeterminable’. The commission also clarified that audits aren’t required for any company under this law unless the company voluntarily chooses to describe any product as ‘DRC conflict free’ in its Conflict Minerals Report, which must be annually publicly filed by most companies subject to the law.

EU proposal creates opportunity

“The US and EU conflict minerals and responsible sourcing laws can put a corporation’s reputation at risk – but they may also create opportunities for a business to open new markets.”

The dynamic US law is no longer alone in the global conflict mineral regulatory field. The EU has published a proposal for “supply chain due diligence self-certification of responsible importers of tin, tantalum, and tungsten, their ores, and gold” – the same ‘conflict minerals’ identified in the US law. The EU proposal is expected to move forward with strength later this year.

While voluntary, the EU initiative may have a wide impact on companies operating in the EU or the
The common thread: supply chain risk management

More importantly, the EU proposal is yet another signpost encouraging companies to develop and internally promote vigorous supply chain and product compliance programs that effectively engage supplier networks to gain needed information. Successful supply chain risk management programs capture, comprehend and communicate necessary information about products, raw materials, processes and packaging throughout the supply chain to help ensure regulatory compliance and protect brand reputation. It has become vital to establish expectations and relationships with suppliers that meet compliance needs without undue resistance. To succeed in this new supplier engagement reality, education, outreach, training and responsiveness become valuable habits.

Optimising due diligence

Companies seeking validation under the EU or US schemes must adhere to the Organisation for Economic Co-operation and Development (OECD) Due Diligence Guidance (OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas), which involves meeting many specific responsibilities under the following broad categories: (i) establish strong company management systems; (ii) identify and assess risks in the supply chain; (iii) design and implement a strategy to respond to identified risks; (iv) carry out independent third-party audit.
of refiner’s due diligence practices; and (v) report annually on supply chain due diligence.

In practice, this means a company may have to make a large capital outlay, coordinating across departments that may not normally work hand-in-hand. To meet the OECD standards, concrete actions need to be taken. Those could include compiling and sorting through a complete list of suppliers; determining which are likely to sell products that contain conflict minerals; developing a supplier communication and engagement plan; collecting evidence of due diligence and verification of claims made by suppliers; revising supplier on-boarding requirements; and establishing contingencies for non-responsive suppliers. Other possibilities include corrective action management or reconsidering business with ‘at risk’ suppliers. Many companies have also established contract flow-down clauses and integrated due diligence policies into standard operating procedures.

To support this type of approach, it is critical to have an adaptive internal or third-party system to collect and manage the essential data. The system must also be accessible to multiple departments in the company.

Data collected for supply chain due diligence exercises can be extremely valuable across the company. Moreover, the system of communication and record-collection established for conflict minerals compliance, if done right, may ultimately be leveraged and used on a greater scale to meet other compliance and risk management goals.

Many companies have viewed these responsible sourcing compliance obligations as a burden. However, companies may alternatively embrace the requirements – risk assessment of the supply chain, inter-departmental cooperation, and supplier outreach – as a rare opportunity to revamp compliance and corporate due diligence programs.

Building a new competitive advantage

Companies from downstream to upstream are wise to invest early in building a conflict minerals compliance program. Truly savvy businesses will build one that can easily adapt and scale to meet other supply chain risk management goals.

Investing the time and human capital needed to establish a comprehensive system that can adapt to the changing demands of regulations and customers can enhance corporate reputation as well as the bottom line. Given the reality of growing supply chain traceability and responsibility regulations, that investment could pay off for years to come. RC

Kirsten Wallerstedt
Senior Regulatory Analyst
3E Company
E: kwallerstedt@3ecompany.com
MINI-ROUNDTABLE

INTERNATIONAL CARTEL ENFORCEMENT
PANEL EXPERTS

Scott Hammond is a co-chair of the Antitrust and Competition Practice Group at Gibson, Dunn & Crutcher, LLP. Mr Hammond is internationally recognised by senior competition officials and private practitioners as one of the leading figures behind the globalisation of cartel enforcement. Before joining Gibson Dunn, Mr Hammond served for eight years as the highest-ranking career official at the Antitrust Division of the US Department of Justice.

Scott D Hammond is a partner at Hogan Lovells International LLP based in London and specialising in EU and UK competition law. He advises on antitrust investigations and compliance, merger control clearances, and market reviews. Mr Jones’ experience includes a secondment to the UK competition authority. He is a recognised competition specialist in the legal directories.

Mark Jones is a partner at Hogan Lovells International LLP based in London and specialising in EU and UK competition law. He advises on antitrust investigations and compliance, merger control clearances, and market reviews. Mr Jones’ experience includes a secondment to the UK competition authority. He is a recognised competition specialist in the legal directories.

Heather Irvine is the head of the Norton Rose Fulbright African competition law team based in Johannesburg. She has been involved in some of the most high profile competition law cases in South Africa since the Competition Act came into effect, including two applications to the Constitutional Court. She is currently advising on a dawn raid conducted by the Zambian Competition Authority. Ms Irvine advises on regulatory issues in the telecommunications and energy sector, including recent High Court review applications dealing with ICASA’s regulation of wholesale mobile call termination rates and NERSA’s recent determination on the maximum charges for piped gas by Sasol Gas.

Heather Lamberg Kafele is a partner in the Antitrust and Litigation Groups in Shearman & Sterling LLP’s Washington, DC office. She has extensive experience in complex litigation, investigations, and regulatory proceedings with a particular emphasis on complex antitrust, competition and consumer issues. She has represented plaintiffs and defendants in a variety of antitrust cases, including monopolisation, price-fixing (cartel), predatory pricing, bundling, tying, false advertising, unfair competition and leveraging cases in state and federal courts across the country. Ms Kafele has extensive experience in representing clients in cartel matters. Ms Kafele has handled worldwide internal investigations of cartel activity.
RC: To what extent have you seen an increase in international cartel enforcement in recent years? In what ways are governing bodies ramping up their efforts in this area?

Hammond: The landscape for international cartel enforcement has changed dramatically in recent years. The changes stem from a near universal consensus among competition enforcers that international cartels inflict substantial harm and that stronger sanctions are required to deter cartel activity. This has led many jurisdictions to amend their competition laws to replace administrative penalties with criminal sanctions for cartel offences or to raise existing maximum penalties for individual and corporate offenders. As a result, cartel members face the prospect of being simultaneously investigated by multiple jurisdictions seeking to impose ever-increasing, and sometimes overlapping, sanctions. The risk of detection has also risen in parallel with the rising penalties. Competition enforcers have made huge strides in their ability to detect and prosecute international cartel activity even when the cartel activity occurred outside of a jurisdiction’s national borders. Enforcers around the world are deploying a similar voluntary disclosure program to encourage companies to simultaneously report international cartel activity in exchange for immunity wherever they face exposure to sanctions.

As a result, it is now no longer unusual for up to 10 or more jurisdictions to simultaneously launch investigations of cartel activity as a result of leads generated by a common immunity applicant. This has contributed to a network of enforcement among competition enforcers resulting in greater coordination and information sharing. The upshot being that the risks and costs associated with engaging in international cartel activity have never been greater.

Jones: There has been a continuing trend of increased cartel enforcement worldwide, as the recent track record of fines levied against cartelists by competition/antitrust agencies around the world shows. In the EU, for example, total cartel fines were at a similarly high level in 2013 as in 2012 – at approximately 1.9bn. Competition authorities have looked to improve their enforcement toolkit on a number of fronts, including greater international cooperation between themselves; increased criminalisation of cartel activity; more extensive deployment of investigatory powers such as dawn raids; and more effective procedures to uncover and prosecute cases through, for example, leniency and settlement regimes which use the prospect of immunity from or reduction of fines to incentivise companies which have been involved in cartels to come forward with evidence of them and admit liability.
Irvine: Competition authorities around the world are increasingly tackling global cartels in a coordinated way, by increasing communication between authorities on investigations, both formally and informally, and coordinating ‘dawn raids’. Investigations in one jurisdiction frequently spark similar investigations in another jurisdiction. This is particularly true in Africa, where relatively new competition authorities such as those in Namibia and Botswana leverage off the experience of the more established South African Competition Commission in order to identify sectors of the economy likely to be prone to cartels, and to combat practices which harm consumers such as price fixing and bid rigging.

Kafele: The past several years have seen record fines issued by ‘core’ competition enforcement jurisdictions like the US and EU, as well as rapid growth in the number of countries pursuing and enforcing anti-cartel statutes. Increasingly, cartel investigations are characterised by extensive international cooperation. At least nine separate enforcement agencies coordinated with the US Department of Justice (DOJ) during the course of the ongoing auto parts investigation, and as many as 10 separate agencies are currently investigating the alleged LIBOR rigging conspiracy. These cross-border investigations have resulted in record penalties, including over $2.25bn in fines to date from the auto parts cases alone. Jurisdictions outside the US and Europe are also stepping up their enforcement activity, with many now pursuing criminal prosecution against price-fixing activity that was previously categorised as a civil offence. In Korea, the Financial Telecommunications & Clearings Institute (KFTC) is now frequently recommending criminal prosecution against individuals as well as against companies. Similarly, Japan has a criminal cartel case pending. Brazil’s enforcement agency has also increased its activity level in the wake of recent legislative reforms, and in 2014 imposed record fines of almost $1.4bn on participants in a cement cartel.

RC: Could you highlight some of the recent international cartel cases of note? How were these cases concluded,

“Cartel members face the prospect of being simultaneously investigated by multiple jurisdictions seeking to impose ever-increasing, and sometimes overlapping, sanctions.”

Scott Hammond, Gibson, Dunn & Crutcher LLP
and what impact will they have on the market?

**Jones:** The spotlight has been firmly on the financial sector in the continuing fallout from the financial crisis. The European Commission fined eight banks €1.7bn for manipulation of the LIBOR and Euribor benchmarks, while UBS and Barclays received immunity for whistleblowing, allowing them to escape fines of €2.5bn and €690m respectively in each of the two cartels prosecuted. These cases were concluded using the settlement procedure. The European Commission is continuing to investigate a number of other banks which did not settle. There has also been enforcement activity by authorities in other jurisdictions. Investigations or allegations of manipulation of benchmark fixes in forex and gold markets have followed around the world. The automotive industry is another sector feeling the heat from anti-cartel enforcement, with the ongoing worldwide autoparts investigation. In the EU wire harness suppliers were fined €142m last year – with Sumitomo whistleblowing to avoid a fine of €291m – and there were also large fines in the US and Canada. This year has seen further fines of €114m in January in relation to polyurethane foam used in car seats and €953m in March in relation to automotive bearings. The Commission is also investigating other automotive components, such as airbags, seat belts, thermal systems for cars and lighting systems. On announcement of the most recent automotive parts cartel decision, it said that more than 100 products and more than 70 companies were being or had been investigated. Again, there are parallel investigations in other jurisdictions. The decisions in both EU cases were concluded using the settlement procedure. In fact, the settlement procedure was been used in all three of the four cartel decisions in 2013 and has been used in four of the five decisions this year. It is therefore very much the new norm, and initial concerns that the level of discount offered, at 10 percent, was too low to incentivise settlement appear unfounded. Both the financial markets and car parts investigations

“Several recent cartel cases have shifted the landscape of potential liability for corporations and individuals.”

Heather Lamberg Kafele, Shearman & Sterling LLP
clearly herald a major shake-up in these industries. In the banking sector, these practices appear closely linked to the conventions of benchmark fixing and the manipulation alleged also raises issues under financial services regulatory supervision. It can be predicted that a more structural response through additional regulation and reform of benchmarking practices will follow. The autoparts investigations, on the other hand, fall into the more traditional category of classic cartel conspiracies, albeit on an unprecedented scale.

**Kafele:** Several recent cartel cases have shifted the landscape of potential liability for corporations and individuals. In April 2014, the DOJ announced that it had succeeded in obtaining its first-ever extradition of a foreign executive to face criminal antitrust charges in the United States. The DOJ’s success in persuading a German court to extradite the defendant in question, former marine hose executive Romano Pisciotti, may further embolden US efforts to prosecute cartel participants who reside outside of US jurisdiction. In contrast, a US 7th Circuit decision issued in March 2014 appears to limit the extraterritorial reach of US law, holding that that the Sherman Act does not reach foreign price fixing of foreign components sold to foreign subsidiaries that are later integrated into finished products that are eventually imported to the US. The decision, *Motorola Mobility LLC v. AU Optronics*, is part of the ongoing fallout from an alleged conspiracy to fix the prices of LCD panels used in notebook computers and smartphones. The 7th Circuit’s decision could have far-reaching consequences on the numerous criminal investigations and civil cases directed at alleged cartels involving components sold overseas and reaching the US as finished products. In today’s global economy “[n]othing is more common nowadays than for products imported to the United States to include components that the producers had bought from foreign manufacturers”. Given the importance of this issue, the United States has filed briefs expressing concerns about limiting the global reach of the antitrust and, by contrast, the governments of Korea, Japan and Taiwan have filed briefs expressing concerns about expanding US antitrust law and international comity. In light of the importance of these issues and inconsistent positions with the court and among governments, this issue will likely be teed up for review by the US Supreme Court.

**Irvine:** Two recent global cartel investigations involve financial services and automotive components. Both are still ongoing and likely to keep various competition authorities around the world occupied for some time. Another notable global cartel case which is still being investigated in South Africa is the pure car carrier investigation. These cases highlight the high level of risk which cartel investigations pose to companies that
operate in multiple jurisdictions, and the need for a comprehensive global competition law compliance program.

Hammond: The parallel ongoing investigations by numerous competition enforcers of auto parts suppliers highlight the seriousness of the sanctions being imposed in international cartel cases and the level of existing coordination among enforcers. The US DOJ alone has prosecuted 27 companies and 35 individuals to date. Corporate fines have exceeded $2.3bn and 22 individuals have been sentenced to serve time in US prisons ranging from one to two years, and the matter remains ongoing. Other jurisdictions are expected to follow with their own sanctions. Moreover, the companies face direct and indirect purchaser class action private damage actions in the United States, as well as other lawsuits in the United States and abroad. It is also noteworthy that when the US Attorney General announced the simultaneous filing of cases against multiple defendants last September, he revealed that the Department had coordinated closely in the investigation with a number of jurisdictions, including the Japanese Fair Trade Commission. Of particular significance was the revelation by the Department that the Japanese authority was the first to detect some of the wrongdoing that led to the US prosecutions.

RC: Do you expect to see a rise in cartel-related class actions? What settlement strategies are being utilised in these cases?

Irvine: Cartel-related class actions should increase. The South African courts recently confirmed in the Pioneer – bread cartel – case that class actions are available to customers who suffer a loss in competition law cases. We are accordingly likely to see more private enforcement actions in South Africa, in line with the trend in the United States and Europe. The bread cartel damages case is currently being litigated in South Africa.

Kafele: The number of cartel-related class actions tends to track the DOJ’s enforcement activity – since civil cases are typically filed in connection with criminal guilty pleas. Given that the DOJ’s ongoing auto parts cartel investigation is the largest investigation ever with more than 26 companies pleading guilty, it is not surprising that the number of cartel-related class action lawsuits has increased in recent years. In addition to an increasing number of class action cases we are also seeing more customer cases. Some of the recent corporate plea agreements have identified by name the victims – that is, the customers – of the alleged cartel. In turn, those customers are, in some cases, electing to pursue remedies outside of the traditional class-
action process, through early settlement or by filing their own lawsuits. For example, in the auto parts cases, Ford Motor Co. has filed a lawsuit against some of its suppliers. Similarly, in the LCD civil cases, Best Buy Co. and T-Mobile filed their own lawsuits. While it may have been unheard in the past for companies to sue their suppliers for price-fixing, that is no longer the case. These companies appear to believe they can extract better remedies outside of the class system.

Hammond: The US model for private damage actions, which allows in certain cases for victims of cartel activity to initiate class action lawsuits seeking treble damage recoveries, remains largely unique. Many jurisdictions around the world allow for private damage actions, but they do not permit either class action lawsuits or the recovery of treble damages for any harm suffered. Most jurisdictions with rights of private recovery rarely see their provisions utilised. A number of jurisdictions are in the process of evaluating the efficacy of their systems for private rights of recovery, with the closest scrutiny currently taking place in Europe. The European Union as well as several member states have been promoting the development of private rights of action at a
national level against infringers of EU competition law. Companies that expect to face an enforcement action by the European Commission will want to consider potential private action exposure in Europe as part of any integrated global settlement strategy.

Jones: This is an increasing trend outside North America, where it has been a risk faced by companies violating cartel laws for some time. In Europe, the European Commission is pushing through reforms to encourage private enforcement of competition law and has also adopted a recommendation which encourages member states to set up collective redress mechanisms, including class actions, by mid-2015. This would be on the more restricted opt-in basis, where claimants have to proactively take steps to join the claim. In the UK, however, reforms are being pushed to allow the possibility of opt-in claims as well, where claimants within a class are automatically included in an action unless they take steps to opt-out. There is already significant class action activity in some European countries such as the UK, where numerous claims have been brought, although most have settled before trial. The high proportion of settlements indicates it as the preferred route for resolution by both claimants and defendants in order to avoid the expense and uncertainty of court proceedings.

RC: What legal and regulatory developments have shaped enforcement activity? Do you expect any further anti-cartel laws in the immediate future?

Kafele: Perhaps the most significant recent trend is the rapid increase in the number of international jurisdictions with criminal antitrust laws on the books. The US Department of Justice has actively sought to promote the adoption of criminal antitrust laws by other countries, with significant success. Australia, the United Kingdom, Brazil, Japan, Ireland and Germany are among the jurisdictions which have adopted or strengthened their criminal antitrust statutes in recent years. In the United States, recent discussion has centred around measures to further increase incentives for individuals to report cartel activity. For example, the Criminal Antitrust Anti-Retaliation Act (CAARA), which has passed the Senate and is awaiting a vote in the US House of Representatives, would provide a private cause of action for whistleblowers who report antitrust violations and experience retaliation. While some have also proposed adding bounties or payments as an additional incentive for individuals to report wrongdoing, no such proposal is currently under serious consideration. Another important US development in the DOJ’s announcement that it will no longer publicly name the executives excluded from immunity granted in corporate cartel plea agreements, but these names will be filed under seal with the court. This policy change is more consistent
with principles of grand jury secrecy and better protects uncharged persons privacy and reputational interests.

Hammond: The development with the greatest impact on anti-cartel enforcement is the widespread adoption of similar corporate immunity – also known as corporate leniency – programs by competition enforcers around the world. Corporate immunity programs have led to the detection of the vast majority of the international cartels prosecuted in recent years. These voluntary disclosure programs promise a full pass from prosecution and other benefits to the first company to come forward and report cartel activity. The transparency, predictability and benefits associated with these programs are unique to competition violations and not offered by government authorities in the United States or elsewhere to companies reporting other financial offences. In the face of rising antitrust sanctions, companies that detect cartel activity before enforcers are taking advantage of these benefits and seeking immunity in exchange for self-reporting. Enforcers open up their leniency programs to virtually everyone, regardless of their role in the offence, with one catch: you have to be the first in the door to report. The need for speed places a premium on the importance of implementing effective compliance programs that will lead to early detection of cartel activity even if the wrongdoing is not prevented in the first instance.

“Increasing numbers of countries adopting or strengthening anti-cartel laws is a clear trend.”

Mark Jones, Hogan Lovells International LLP

Jones: Increasing numbers of countries adopting or strengthening anti-cartel laws is a clear trend. We have talked about the spread of criminal sanctions and leniency regimes already. Another development of note in the EU has been several European court cases clarifying the extent of liability of parent companies for competition law breaches by subsidiary companies. Generally the approach has been to establish liability in view of the responsibility exercised by the parent. In one case concerning a cartel in subsea cables, liability was attributed to a private equity investor, Goldman Sachs Capital Partners, in relation to its portfolio
company, Prysmian. The position was considered no different to that of a parent and subsidiary in a corporate group in that Goldman was found to hold decisive influence in the company and therefore be liable. The most significant development in the EU, however, has been the promotion of private enforcement in the courts and collective redress through class actions. An EU Directive on antitrust damages is expected to be finalised shortly. This will improve the ability of claimants in litigation to rely on infringement decisions taken by competition authorities so that they just need to claim for compensation of their loss – so-called follow-on claims. The reforms also seek to improve and harmonise procedure to a greater extent, while seeking to avoid undermining the incentives of to cooperate in investigations by competition authorities by limiting the scope for disclosure in litigation of evidence provided to the authorities.

Irvine: Globally, an increasing number of competition authorities have introduced corporate leniency policies in order to incentivise cartel insiders to disclose the cartel in exchange for substantial cooperation and immunity from penalties or reduced fines. These policies have improved the ability of authorities around the world to detect and prosecute cartels, and they have also led many companies accused of cartel conduct to settle cases by paying a fine, rather than engaging in costly and protracted litigation. In Africa, a number of relatively new authorities have recently begun to tackle cartels, including Zambia, Namibia and Tanzania.

“Companies need to institute a comprehensive global competition law compliance training program, which is adequately tailored to the law in each jurisdiction in which they operate.”

Heather Irvine, Norton Rose Fulbright South Africa

RC: What advice can you offer to firms on managing and mitigating the risk of violating anti-cartel laws around the world?

Hammond: Horizontal agreements among competitors to fix prices, rig bids or allocate customers and markets are unlawful just about everywhere. It is only the penalties and the risk of detection that varies depending on the jurisdiction. As a result, companies operating internationally should adopt a code of conduct prohibiting cartel
behaviour wherever the company does business. The challenge for any multinational company operating in various jurisdictions around the world is converting its code of conduct into a culture of compliance that permeates its entire business. This can be especially problematic for businesses operating in markets where competition offences have traditionally been seen as akin to ‘gentlemen’s agreements’ or where competition authorities are perceived as weak and the risk and costs of detection minimal. Particularly problematic is the scenario in which cartels are operating in jurisdictions where antitrust compliance and enforcement are viewed as soft, but those same businesses are selling into markets that take a hard line on cartel activity and apply their laws with a broad extraterritorial reach. There are many non-US business executives presently serving time in US prisons who were tripped up by that false sense of security.

Jones: Many countries now have cartel laws – around 50 at least. These rules can quite often be effects-based, where competition authorities will seek to assert jurisdiction if there is an impact on markets and customers in their territories because the goods or services in question are sold there, even if the parties or the infringing activity was not located there, which gives these regimes a long reach. In addition, competition authorities around the world liaise closely through a variety of formal and informal channels. Particularly for multinational businesses, therefore, the chances are that any cartel investigation will be multi-jurisdictional and create a number of challenges in terms of dealing with different procedures and timescales, different rules on leniency and settlement of cases, and different levels of exposure to related litigation claims. All of this makes it important to have an effective compliance program in order to create a compliance culture at all levels and in all areas of the business across the territories in which it operates. That said, there will be a balance to be struck between prudent and clearly understood policies applicable worldwide and unnecessary restriction of commercial activities.

Irvine: Companies need to institute a comprehensive global competition law compliance training program, which is adequately tailored to the law in each jurisdiction in which they operate. Staff at all levels need to be trained on competition law compliance, and proper measures for detecting and reporting potential concerns must be put in place globally.

Kafele: The most important step a company can take is to develop an antitrust compliance program early on and to ensure that employees receive regular, relevant training. A good compliance program will be tailored to the location and nature of a company’s business and will pay special attention to those employees and business units
whose duties put them most at risk. Key objectives include building a culture of antitrust awareness, honing employees’ intuitions, identifying antitrust red flags, and encouraging employees to report their suspicions to in-house counsel. Compliance planning also allows firms to prepare appropriate responses in the event that the firm comes under scrutiny or discovers inappropriate behaviour, including procedures to follow during dawn raids and plans to limit corporate exposure in the event of bad conduct by an individual employee.

RC: In your experience, what are the first steps a company should take when it learns it is being investigated for possible cartel-related activity?

Jones: If the first that the company hears about the investigation is in the form of competition authority officials turning up unannounced to conduct a dawn raid, there are a number of basic initial steps that should be followed, including checking the officials’ authorisation documents to understand the nature and scope of the investigation; contacting external competition counsel and ideally seeking to delay the start of the investigation until they arrive; ensuring that staff understand their obligations to cooperate with officials, such as not to destroying any business records or communications, but also the limit of the officials’ powers which do not include looking at legally privileged material; and preparing an external communications strategy. If the investigation becomes apparent through receipt of a written request for information, then there is scope for a more measured approach. Particularly if a company fears it may be investigated – perhaps because anti-competitive practices have come to light through internal reporting, or it is known that there is a cartel investigation being conducted in the markets in which the company operates albeit that the company itself has not yet been contacted by the authorities – a key consideration will be to decide whether it has breached cartel laws and, if so, whether it is worth applying for leniency. This may include whistleblowing by cooperating with the authorities through the production of incriminating evidence in return for immunity from or a reduction in fines.

Kafele: The first step is always to notify counsel. The company and its counsel then must quickly determine which jurisdictions the alleged cartel-activity may have impacted, and mobilise to investigate so the company can promptly determine whether to seek leniency and in which jurisdictions. The most frequent mistake is moving too slowly because the company wants to do a thorough investigation before reporting to authorities. But remember amnesty can be lost in a matter of days or even hours. Time is of the essence in this initial investigation. If you uncover a violation, the
company should immediately evaluate whether to seek leniency. A more detailed investigation can come later. The second most common mistake is not appreciating all of the jurisdictions that may be involved. Enforcers other than the US and Europe are active and companies need to retain local counsel in those jurisdictions and consider seeking leniency. Key employees, including IT staff, receptionists and managers, should already have received training. Employees should be reminded quickly that they may answer investigators’ questions, but that they do not have to and that they have a right to have a lawyer present during interviews. Above all else, a company should never obstruct investigations or destroy records – doing so can lead to criminal charges. Sometimes, a dawn raid or a search warrant is the first indicator that a company is being investigated. In such a case, companies should notify external counsel immediately and make copies of inspectors’ identification cards and legal authorisation. Among other things, counsel should shadow inspectors to facilitate the search, take detailed notes, and object to searches outside of scope or violating privilege.

**Irvine:** It is critical to engage external counsel with substantial antitrust experience at an early stage in order to ensure that a full investigation can be carried out in a manner which adequately protects the company and puts it in the best possible position to deal with global competition authorities.

**Hammond:** When a company learns that it is under investigation it must move quickly and simultaneously on many fronts. The key to executing these steps quickly and effectively is advance preparation. Ideally, the company will already have trained its employees on the proper protocol in the event of a government investigation, so its employees will know how to respond if FBI agents knock on the door of their homes at night or show up at the office waving a search warrant. Proper advance training is crucial at these moments as it is rarely the case that the company’s legal representatives will be present when the government first takes its investigation overt. It is also critically important that a company know who it will secure for its legal representation in the event it is the subject of a cartel investigation before agents are streaming through the front door. If that relationship has not already been established, the company will likely find itself represented by counsel operating outside of his or her area of expertise while the company loses valuable time shopping around for proper counsel. And make no mistake, moving quickly in the early stages of a government investigation, especially cartel investigations, is critically important to preserving the company’s opportunities for lenient treatment. The US DOJ, as well as the rest of the world’s other major competition authorities, offer a unique immunity program available to the first company to come forward and admit wrongdoing. In the first contact
with the prosecutor, company counsel should inquire as to whether the immunity position is still available. If it is, then the company needs to move as expeditiously as possible to determine whether it is at risk to determine whether it should seek a marker for immunity. Simultaneously, it must take appropriate steps to preserve relevant electronic and documentary evidence to ensure that its exposure to sanctions is not compounded by employees either wilfully or negligently destroying evidence.

**RC: What advice do you have for in-house counsel on managing anti-compete allegations? What benefits can companies derive from engaging external counsel to assist the process?**

**Irvine:** It is never too early to seek assistance from global counsel. Ideally one needs a law firm with substantial experience in all of the major jurisdictions around the world, so that the investigation can be pursued as swiftly and efficiently as possible. In-house counsel should ensure that they have strong relationships with their external lawyers who know and understand the business in order to place them in the best possible position to deal with an investigation.

**Hammond:** Experienced outside counsel can assist in-house counsel in designing an effective corporate compliance program to reduce the risk that its employees engage in cartel activity and that wrongdoing is quickly detected in the event it occurs. When questionable conduct arises or the company finds itself operating in a grey area, in-house counsel should have ready access to trusted counsel who can provide an informed opinion as to whether the government is likely to view the conduct as a violation and, if so, whether it should be reported. In-house counsel will also find it useful to bring in experienced external counsel so that the board of directors or others will have confidence that key decisions are made impartially, particularly where high-ranking executives may be potential subjects of an investigation and their interests may not always be perfectly aligned with the company’s.

**Jones:** So far as dawn raids are concerned, the best approach is to ensure that the business is prepared for this through training and implementation of procedures to use in the event that a raid occurs. More fundamentally, an effective compliance program and internal reporting procedures help to prevent anti-competitive behaviour in the first place or at least manage it promptly and effectively where it has occurred. Where allegations are made, it will be important to undertake an internal review; manage the staff involved; report to senior management; assess what steps are needed to bring any infringing conduct to an end and prevent further breaches; decide on whether to approach the competition authorities...
for leniency; and generally develop a strategy for managing the potential exposure to liabilities which will often be across different jurisdictions and involve the risk of litigation claims for damages as well as enforcement action by the authorities. External competition/antitrust counsel can bring greater specialist experience to bear in dealing with these issues, including representing the company before the competition authorities, as well as additional resources to support the company in what are usually labour-intensive exercises. A particular advantage of using external lawyers in the EU is that communications with external EU-qualified counsel benefit from legal privilege, meaning they are not disclosable to the authorities, whereas communications with in-house lawyers do not.

**Kafele:** Allegations of anticompetitive behaviour should be analysed immediately, including the availability of leniency, if appropriate, and the likelihood of enforcement by public authorities. Time is of the essence, since leniency in most jurisdictions is only available to the first company to apply. Given the enormous scale of recent antitrust fines and judgments, engaging external counsel early is a key component in managing risk. Experienced counsel can assist in assessing the evidence, weighing the available options, plotting a strategy to minimise harm to the firm, and coordinating a global response. The need for outside help has become even more urgent with the trend towards increased international enforcement, since any given company is likely to face a multiplicity of potential enforcers, and the decision to cooperate with or respond to any given set of authorities will have potential implications for civil and criminal liability worldwide.

**RC**
any of the legal risks in international business revolve around the concern of whether a dispute will be fairly and timely resolved in a foreign country. Individuals and companies seeking to conduct business abroad can mitigate such risks by wisely selecting the governing law and forum provision that will protect their conduct of business in each foreign country. Fortunately, there are only two main options to choose from: (i) arbitration under an internationally known arbitration law and body; and (ii) a foreign court under foreign law. This article analyses each option, provides tips for ensuring the option selected is written in a manner that is enforceable, and explains the importance of permitting injunctive relief so that a court can quickly stop a party from causing harm until a final and binding decision on a dispute is obtained.

Both arbitration and a foreign proceeding have their advantages and disadvantages, and neither option is necessarily the best choice in every situation. To determine the best choice, each of the following issues must be analysed: (i) the predictability of judicial decisions (including the corruptness of the judiciary); (ii) the length of time it will take for an arbitral or judicial decision to be made within the country; (iii) the costs for obtaining an arbitral or judicial decision; (iv) whether a decision
is appealable; and (v) the enforcement of a judicial or arbitral decision both from within the foreign country and outside the country.

The modern trend has been for arbitration to be the default choice in international business, but while proponents of arbitration are adamant that it is always the best option, companies should recognise that arbitration is often just as costly and time consuming as a judicial proceeding. Furthermore, arbitrators are not required to follow any precedence of legal decisions, and this permits them to resolve matters in an unpredictable manner. Judicial decisions, on the other hand, are intended to follow legal precedence, and this allows counsel to better predict the decision and determine a party’s best strategy for obtaining a favourable decision. Moreover, an arbitral decision is not appealable. Therefore, if the arbitrators came to an incorrect decision, there is no course of correction. In contrast, judicial decisions are typically appealable.

That said, arbitration does have the benefit of skirting past the kind of biased, unpredictable or slow judicial process that is found in many countries throughout the world. This can occur if the foreign country of each party to an agreement is a member of the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards, in which case enforcement of an arbitral decision should be
simple and quick. Once arbitration is completed in a member country, the parties simply must provide a copy of the decision to the foreign court which in turn is required to strictly comply with and enforce the decision.

After weighing the above factors and coming to a decision, perhaps the most difficult part follows: ensuring the governing law and forum provision is written to be enforceable. The selection of a foreign court and forum is easy to implement. Merely write the name of the foreign country and court into the company’s standard governing law and forum provision, and adjust the language accordingly as it would be adjusted if a different state, province or county within a company’s own country were selected. Arbitration, in contrast, is much trickier and often written incorrectly. The provision must expressly state each of the following aspects, and if any one aspect is not sufficiently clear, then a foreign court could decide not to enforce an arbitral decision and circumvent the entire provision by having a foreign proceeding. The key aspects are: (i) that the agreement to arbitrate is final and binding; (ii) that the entire agreement is subject to arbitration; (iii) the set of rules and administering body for the arbitral proceeding (UNCITRAL, the American Bar Association, or another internationally reputed body); (iv) the number of arbitrators (this should always be an odd number to prevent a stalemate); and (v) the language of arbitration.

The attention to detail does not end there. In addition, the arbitration provision must be ‘localised’ to the foreign jurisdiction in which it is intended to be enforced, and often ‘magic language’ must be inserted to ensure it will be enforced. The perils of not localising can be seen from India, a common law country with a sophisticated legal system and a common destination for international business, but known for its slow judicial decisions. Unless the provision expressly disclaims Section 34 of Part 1 of India’s arbitration act, then a foreign arbitration award is likely appealable, and the decision making body would not be a panel of arbitrators and instead would be an Indian court. However, if the arbitration provision is written to expressly disclaim such section, then a foreign award must be enforced by the Indian court provided all parties

“Legal risks are abundant in international business, but can be significantly reduced by ensuring that the governing law and forum provision are correctly selected and written to be enforceable.”
to the agreement are members of the New York Convention. Without this short sentence, the entire decision to require arbitration could easily be evaded.

After selecting whether arbitration or a foreign court will be used, it is imperative that the governing law and forum provision allow for injunctive relief. This is an equitable remedy that is an excellent reducer of legal risk because it is used in time sensitive situations by any applicable court, regardless of whether such court is expressly named in the agreement, to require a party to immediately take certain actions, or to refrain from taking certain actions, until a final judgment is entered. Typically, injunctive relief is used to prevent a party from violating a restrictive covenant, such as divulging confidential information, engaging in a competitive activity or making disparaging remarks, or to otherwise prevent harmful activity. Injunctive relief must be permitted for two main reasons: (i) the harm may be occurring in a jurisdiction outside of the exclusive forum selected by the parties, so the agreement should permit any court with jurisdiction over the party causing the harm to seize such activities; and (ii) a decision to temporarily stop the harmful actions should occur through an independent arbitral or judicial decision that is made much earlier than the issuance of a final judgment on the merits of the dispute. If it is not expressly permitted, then an arbitrator or court may interpret the provision’s silence as the intention of the parties to require the exclusive forum to be the sole venue, which would be ineffective if such forum does not have jurisdiction over the party in the location where it is causing the harm, or to disallow injunctive relief altogether. The perils of either outcome are significant since it would allow the injurious activity, such as divulging confidential information or engaging in competitive activity, to continue unabated until a final decision is made.

Legal risks are abundant in international business, but can be significantly reduced by ensuring that the governing law and forum provision are correctly selected and written to be enforceable. Once prepared, this can and should be used for several types of agreements, including each agreement with any international aspect.

Manish Antani
Attorney
Gould & Ratner LLP
T: +1 (312) 236 3003
E: mantani@gouldratner.com
MINI-ROUNDTABLE

ADVICE FOR NON-EU FUND MANAGERS ON AIFMD COMPLIANCE
PANEL EXPERTS

Richard Small
Regulatory Counsel
Davis Polk & Wardwell London LLP
T: +44 (0)20 7418 1379
E: richard.small@davispolk.com

Richard Small is regulatory counsel in Davis Polk’s London office specialising in non-contentious European and UK financial regulatory law matters. He works closely with the Investment Management Group advising alternative investment funds on a wide variety of regulatory issues.

Neil Robson
Special Counsel
Schulte Roth & Zabel International LLP
T: +44 (0) 20 7081 8037
E: neil.robson@srz.com

Neil Robson is a special counsel in the London office, where his practice focuses on counselling hedge and private equity funds on operational, regulatory and compliance matters regarding Financial Conduct Authority (FCA) and EU authorisation and compliance, including under both MiFID and the AIFM Directive, cross-border issues in the financial services sector, market abuse, anti-money laundering and regulatory capital requirements, formations and buyouts of financial services groups and structuring and marketing of investment funds. Mr Robson writes regularly on regulatory matters for various professional trade publications and has authored many client communications pieces.

Hilger von Livonius
Partner
King & Wood Mallesons LLP
T: +49 (0) 89 89081 238
E: hilger.vonlivonius@eu.kwm.com

Hilger von Livonius specialises in banking, investment and insurance regulatory matters with a specific focus on investment funds and debt capital markets. He also has expertise in the betting and gaming sector and in commodity funds and funds of funds. He regularly advises: financial institutions on the issuing of financial products, including structuring, documentation and distribution; institutional investors on real estate and alternative investments; banks and other financial intermediaries on general regulatory issues such as licensing requirements and codes of conduct; and on the structuring, documentation and marketing of financial products for the German market.
RC: In brief, could you provide an outline of Europe’s AIFMD, touching on its key functions and the drivers behind its implementation?

Small: The driving force behind the AIFMD was the concern, underlined by the financial crises, that the activities of some fund managers could serve to spread or amplify risks through the financial system and that uncoordinated national responses made the efficient management of those risks difficult. The purpose of the AIFMD was therefore to bring fund managers within the European regulatory umbrella. The AIFMD achieves this by establishing a common set of requirements governing the authorisation and supervision of fund managers. In addition, the AIFMD sets out remuneration rules aimed at aligning fund managers’ interests with those of investors, limitations on leverage and asset stripping, a disclosure regime and rules in relation to the marketing of funds by non-EU fund managers. Fund managers are also required to appoint depositaries for each fund to monitor cash-flows, safe-keep fund assets and have general oversight over the fund. Finally, the AIFMD introduces a pan-European passport under which EU fund managers may market EU funds across the Member States.

von Livonius: The rationale behind the AIFMD, probably one of the most significant legislative projects within the enhanced ‘post Lehman’ financial markets regulation, is to provide a harmonised regulatory framework for the so-far rather fragmented supervisory landscape in Europe. To achieve this goal, the AIFMD introduced a uniform regulatory framework for all collective investment vehicles which are not yet covered by the scope of the UCITS Directive. There is only a very limited number of collective investment structures remaining outside the scope of the AIFMD. However, the AIFMD is more a manager regulation than a product regulation. But the impact of the AIFMD goes beyond the regulation of AIF managers as it also has a significant impact on the regulation of investment activities by regulated investors, such as insurance companies and pension schemes, in AIFs.

Robson: The AIFM Directive regulates the services of alternative investment fund manager operating in the EU/EEA – UCITS fund managers are out of scope as they are covered by the regulations under the UCITS Directives. It requires that EU managers are specially authorised, or licensed, as AIFMs, subject to regulatory capital requirements and a wide range of requirements for the management and marketing of their non-UCITS funds in the EU. However, it also applies to the management and marketing of EU funds, wherever those funds’ AIFMs are established, and the marketing of non-EU funds in the EU – hence many of its provisions may become applicable to non-EU managers, if they are marketing in the EU.
The AIFM was proposed by European lawmakers in the aftermath of the financial crisis as a result of perceived regulatory failings in the EU financial services sector. The lawmakers in Brussels wanted to see regulation of fund managers being more tightly controlled, with much higher levels of transparency and higher regulatory capital buffers in case of insolvency or another financial meltdown.

**RC: What impact do you believe the AIFMD is likely to have on non-EU fund managers operating in the European alternative investment market? Are fund managers generally aware of the requirements imposed by the AIFMD?**

**von Livoniust:** The AIFMD has a significant impact on non-EU fund managers wanting to market their AIFs in the EU as most of them will for the first time face regulation of their activities and the funds which they manage – while certain AIF managers, such as those managing open-ended real estate funds, had, under previous local rules in places like Germany or Luxembourg, already been exposed to a similar level of supervision as the one foreseen for UCITS and are therefore ‘used’ to the regulatory burden, for example the requirement to obtain a manager licence. Some of the relevant requirements need the involvement of other parties, such as depositaries, while other requirements are completely beyond the AIFM’s control – like the requirement for cooperation arrangements being in place between the competent authorities of the Member States where the AIFs are marketed and the supervisory authorities of the third country where the non-EU AIFM is established and, as the case may be, the supervisory authorities of the third country where the non-EU AIF is established.

**Robson:** Non-EU managers operating in the EU will now have to assess where they really want to focus their marketing strategies because before they can become eligible to conduct any marketing they need to register with the relevant regulator – on a country by country basis. Not all countries have registration processes that non-EU managers

“Non-EU managers operating in the EU will now have to assess where they really want to focus their marketing strategies.”

Neil Robson,
Schulte Roth & Zabel International LLP
can actually use; others are highly restrictive and time consuming – such as Germany where our experience shows registration with BaFin can take up to three months and is expensive. However, at the other end of the scale the UK and the Netherlands have flexible registration rules – though this does mean that the manager has to then comply with disclosure obligations including pre-investment disclosures and annual reporting, as well as disclosures to EU regulators – in the AIFMD Annex IV, which is the EU version of the SEC’s Form PF.

Experience with our clients has shown a range of knowledge among non-EU managers, from some who are well versed in AIFMD and are focused on the finer nuances and appreciate that they only want to register in key jurisdictions where they traditionally raise funds, to those who have barely heard of the AIFMD and are shocked to find it exists.

**Small:** The AIFMD has had a disruptive impact on non-EU fund managers seeking to operate in the European alternative investment market. Non-EU fund managers are now broadly aware of the requirements imposed by the AIFMD, however, uneven implementation among Member States has led to a certain level of confusion. Whilst it is too early to have a clear view of the impact of the AIFMD on the alternative investments market in Europe, the response of non-EU managers to the AIFMD and the national private placement regime being put in place by certain Member States will mean that some non-EU managers will no longer be marketing their funds in certain Member States, thereby reducing the range of funds available to investors.

**RC:** In what ways might certain non-EU fund managers need to alter their fund marketing strategies?

“Given the narrow definition of reverse solicitation in many Member States, fund managers should take care to ensure that they have an appropriate audit trail.”

*Richard Small, Davis Polk & Wardwell London*

**Robson:** The simple answer is that non-EU managers cannot simply come on marketing roadshows any more. Registration is required and preparatory filings and PPM updates must be prepared well in advance. Many managers from outside the EU have focused on the reverse
solicitation exemption from AIFMD ‘marketing’, and are deciding not to do any marketing other than where it can be shown to be at the initiative of the EU investor.

**Small:** In light of the obligation to obtain prior approval and, in certain Member States, to appoint a depositary on behalf of each fund being marketed into that Member State, non-EU managers are having to adopt strategies to determine the level of interest in a particular jurisdiction before commencing the approval process and appointing a depositary. Given the broad definition of marketing in most jurisdictions, this is proving difficult in practice. Whilst there is no bright line rule that covers all Member States, it would appear to be broadly acceptable to contact investors with non-fund specific information about the manager in order to determine whether there is a level of interest in that particular manager. To the extent that there is sufficient interest, non-EU managers may then seek prior approval to market their specific funds in that jurisdiction and, if necessary, appoint a depositary. Reverse solicitation is narrowly interpreted in many Member States.

**von Livonius:** Prior to AIFMD implementation, the marketing of AIFs was in many jurisdictions governed only by local placement regimes which also foresaw the possibility of a private placement – a distribution activity which was only addressed to a limited number of investors, sometimes also combined with substantial minimum investment amounts. Post AIFMD implementation, countries like Germany have given up their previous private placement regimes such that only so-called ‘reverse solicitation’ scenarios remain outside the scope of regulated distribution activity, while details of what constitutes such a ‘reverse solicitation scenario’ are as yet unclarified. Any other marketing activity needs to account for the requirement of prior notification of the relevant AIF with the competent authorities of the Member States where the AIFs are marketed. Furthermore, non-EU fund managers should have an eye on local licensing requirements for distributors which they use.

**RC:** What new compliance challenges will the AIFMD present to non-EU fund managers? How is this likely to affect backroom functions?

**Small:** Non-EU fund managers will need to put appropriate systems and controls in place to ensure that when communicating with European investors, they are not characterised as marketing, thereby triggering the prior approval and depositary requirements. Given the narrow definition of reverse solicitation in many Member States, fund managers should take care to ensure that they have an appropriate audit trail so they can demonstrate to the competent authorities that it is reverse solicitation. A letter or email of attestation from the
prospective investor setting out the circumstances in which the prospective investor approached the non-EU manager would help in this regard. The disclosure and reporting requirements also present challenges.

**von Livonius:** Among the various ‘compliance burdens’ imposed on AIFMs are those on initial capital and own funds requirements, on regular detailed reporting to supervisory bodies, depending on the amount of AuM, on the establishment of an independent risk management function, which is separated from other operational functions, and the requirement for a depositary. They have a significant impact on the setup of fund managers and, in particular, on the ongoing administrative costs. But the new regulatory framework also creates new business opportunities for those offering ‘back room functions’ on a professional basis for funds and their managers.

**Robson:** Non-EU managers that register need to confirm that their funds PPMs comply with AIFMD mandatory disclosures, that the fund being marketed in the EU produces an annual report document within six months of the fund’s financial year-end, including disclosures as to the manager’s compensation, both paid to the manager by the fund and paid by the manager to its staff. Also, non-EU managers which register in EU countries have to comply with the relevant countries’ private placement rules and the countries’ risk reporting requirements under Annex IV, as each country is required by the AIFMD to get the registered manager to file semi-annual or quarterly reports, which are the EU version of Form PF.

**RC:** In your experience, are non-EU funds prepared to comply with the transparency requirements of the AIFMD, in terms of disclosures and reporting?

**von Livonius:** In our experience some managers underestimated the level of detail in AIFMD legislation, which makes it quite burdensome to comply with transparency and reporting requirements, particularly against the background of approaching deadlines. This applies, in particular, to managers employing complex investment strategies and instruments or leverage. Also, some managers took the approach of using reporting formats which they are already familiar with – but then discovered that AIFMD reporting is not just the same. And there is also some level of uncertainty regarding the use of external service providers to perform the required functions, and sometimes the misconception that a full ‘transfer of liability’ to any such providers can be achieved.

**Small:** Non-EU fund managers are broadly aware of the disclosure requirements – the disclosure requirements to investors at the time of investing, the production of an audited annual report and
regular reporting to competent authorities, as frequently as quarterly – although many are in the process of resolving issues in connection with the timing and level of granularity with which such reports should be made. For example, there are tight deadlines for the production of quarterly reports to competent authorities – for example, within one month of the end of the quarter for most funds and within 45 days after the end of the quarter for feeder funds. Managers will therefore have to put systems and control in place to ensure the timely and accurate production of these various disclosures as well as the ongoing monitoring of disclosures, particularly in respect of side letters, to ensure that disclosures are amended where necessary to keep them up-to-date.

Robson: In our experience there is a high percentage, approximately 75 percent, of non-EU hedge fund managers who do not want to comply with the AIFMD’s disclosure and reporting rules, so many are taking a view, at least in the short to medium term, that they will only market to EU investors who reverse solicit marketing materials from the non-EU manager at their own initiative. Even more private equity fund managers are electing not to register in our experience, principally because of the AIFMD’s asset stripping rules, which require that when a non-EU fund is registered in the EU for marketing, if that fund – either alone or with other funds managed by the same manager, or with other funds under a concert party agreement – takes control of a certain sized EU company it will be subject to requirement not to asset strip or reduce the value for two years thereafter, and to consult with employee representatives and disclose the

“In our experience some managers underestimated the level of detail in AIFMD legislation, which makes it quite burdensome to comply with transparency and reporting requirements.”

Hilger von Livonius, King & Wood Mallesons LLP

manager’s intentions for the company. Many non-EU funds which have an investment strategy focused on the EU simply do not want to get embroiled in these rules, so their managers are not registering, it seems.

RC: What steps can non-EU fund managers take to ensure the structure of their funds are AIFMD compliant?

Robson: Non-EU managers that want to structure funds that are fully AIFMD compliant, and which
therefore get the benefit of the EU cross-border marketing passport, need to ensure that the fund has an EU AIFM entity. Only EU funds with EU AIFMs get the marketing passport at present, although later in 2015 the European Commission may, potentially, extend it to non-EU funds and non-EU managers. One potential workaround in the short or medium term is to sub-advice an EU sub-fund on an EU platform which has an EU AIFM. The AIFM necessarily has to retain risk management over the sub-fund and must supervise the portfolio management, although that portfolio management could be conducted by the non-EU manager. However, depending on what EU country the EU AIFM is registered in, it is possible that the non-EU manager may have to comply with EU compensation rules as, strictly speaking, EU AIFMs are required to ensure that their delegates comply on a contractual basis with the same compensation rules that the EU AIFM itself is; some EU countries have applied this requirement in different ways, so non-EU managers should seek local counsel’s advice.

**Small**: Given the proposed introduction of the pan-European passport for the marketing of funds for non-EU manager from the latter half of 2015 and the proposed withdrawal of the existing private placement regime in 2018 – which will mean that post-2018 the only route by which an investor may invest in a non-EU fund managed by a non-EU manager will be via reverse solicitation – fund managers for whom the EU is a key source of capital should consider re-domiciling or appointing an AIFMD authorised manager to be able to make use of the pan-European passport. Second, in light of the requirement in certain jurisdictions that evidence be provided that the manager of the fund is suitably supervised in its home jurisdiction, some funds structured as limited liability partnerships will need to amend their documentation to the effect that the manager of the fund is appointed by the limited partnership rather than a delegate of the general partner, who is technically the manager, as the general partner will usually not be regulated and as such it would not be possible to provide the required attestation in respect of the general partner.

**von Livonius**: The ‘way to AIFMD compliance’ should start with a thorough evaluation of the manager’s operations and the structure and investment strategy of the AIFs managed. Of course, time is of the essence because managers otherwise run the risk of facing ‘business disruptions’ for not being able to lawfully manage their funds in an AIFMD-compliant manner after the end of grandfathering periods. Sometimes, the ‘light touch’ regulation applying to small AIFMs can be a viable solution for mangers who want to limit the regulatory burden to a reasonable limit, and we noted that some regulators are willing to accepts ‘creative’ structures which retain a lot of flexibility for the relevant manager. Finally, ‘product wrappers’
may be considered as a tool to avoid the burden of AIFMD compliance.

**RC: What final advice can you offer to non-EU fund managers on addressing the AIFMD and operating successfully under its new regime?**

**Small:** Non-EU fund managers should nominate an individual to be a central point of contact for all AIFMD matters. Second, non-EU fund managers should ensure that their staff are fully aware of the marketing restrictions in the EU and systems and controls should be put in place to make sure that only appropriate ‘marketing materials’ are distributed to potential EU investors before approval to market has been obtained. Third, non-EU fund managers should adopt strategies for determining whether there is a sufficient level of interest or not in a jurisdiction before seeking approval to market their fund in that jurisdiction. Finally, non-EU fund managers for whom the EU is a key source of capital should, given the lead time involved, start considering either re-domiciling their manager to the EU or appointing an AIFMD authorised manager in order to make use of the pan-European passport for marketing funds, which should be available from the latter half of 2015.

**Robson:** My final advice would be to engage local counsel in each EU jurisdiction where the non-EU manager wants to conduct marketing. The local laws and rules may all be derived from the AIFM Directive, but there are some significant variations from country to country – including different definitions of common words or concepts – hence local advice is of paramount importance to ensure compliance.

**von Livonius:** We would advise every manager to take some time and do a thorough analysis of its portfolio to assess for which funds it is actually worth undergoing the regulatory burden, and, in particular, the costs of AIFMD compliance. Furthermore, each manager should also consider the specific local needs of its investors, particularly tax and or regulatory implications which raises their expectation that your fund is AIFMD compliant. With regard to the ‘marketing passport’ which will be available in the future, managers should also assess whether it is worth ‘opting in’ and achieving full AIFMD compliance. Finally, managers should not forget to conduct a review of their fund governing documents, including arrangements with external service providers. **RC**
PERSPECTIVES
THE BIGGEST RISK OF ALL: SUCCESS

BY DEBORAH HICKS MIDANEK
> SOLON GROUP, INC.

We live today in a business climate that seems obsessed by the need to identify, quantify, analyse, manage, mitigate and otherwise corral risk in all its forms. While we fight these battles on the risk management front, we might be risking losing the war of survival of the fittest.

Success represents the biggest risk of all. Whether we look at the fall of Rome or the decline of the British Empire, the embarrassment of Fannie Mae, the collapse of the subprime market the first time, the second time, and no doubt the third, the list of such wars lost is long and examples ubiquitous.

In our compulsive, it seems, desire to tame risk, how do we handle this one? How can we tell when what looks and feels like success is actually the beginning of the end? This is a difficult task, as fish cannot see water. Stepping outside of ourselves to try to discern and interpret the augurs requires constant effort, rigorous vigilance, and effective mirrors. And we are trying to do this at the very time when the livin’ is just too easy. The money is rolling in, and it is so much easier just not to think about it. Discipline is a forgotten concept as we revel in rewards. We must be doing something right. Right?

Wrong. At that point, where profits are flowing and we are on top of the world, we are deaf, dumb and blind. What to do? First, a home truth. Anyone, any entity, person, organisation, institution, civilisation can fail and many do, all the time. Everyone is
vulnerable, and never more vulnerable than when at the peak of success. No one is too powerful or successful to succumb. Thus humility is an imperative as we remember that we all put on our pants one leg at a time.

Beyond that, with that scary awareness in place, are there signs in the midst of great success that can be codified that the vigilant can see? Our goal here is not to add another set of boxes to check on the risk management matrix, but to find insight we can use to protect ourselves. No model provides truth; the best they can do is help identify trends, especially those we may not be expecting. The issues are subjective, and every company experiences them differently.

Experience suggests the behaviours below can be indicative not of success but instead markers of the slippery downward slope.
The Deluded. Who has not seen leaders unable to distinguish corporate success from their own? Who find themselves taking success for granted, and developing an insufferable attitude of entitlement? Once that attitude takes root, such people often take on imperial characteristics, which leads to isolation, and then to great danger, for themselves and their organisations. Though they can often coast on momentum for a while, eventually they and their companies pay a terrible price as things go wrong, and the arrogant leader, out of touch and unfamiliar with the fundamentals that drive the company, is ashamed and thus frozen.

The Hyperactive. That arrogance, uncorrected, can lead to misinterpreting information through a lens in which the leader sees himself as invincible and corporate success as a right. In such circumstances, a production at all costs mentality can take hold, causing the constant pursuit of more, via acquisition or driving up volume. The subprime industry, where the drive to securitise more and more loans to support the perception of earnings momentum, driven by ever increasing gains on sale, caused underwriting standards to weaken to absurd levels and the resulting paper therefore to be near worthless provides a great example: the model was working, right? We achieved our earnings momentum, until we stopped literally dead in our tracks. The system’s failure was crystal clear to those watching from outside, but from inside, what had to be done, it seemed, was always more and faster, with ever weaker people in place as the able ones left the treadmill.

The Ostrich. Next comes the river in Egypt, which we all know is Denial. This is when no matter what the data says, the explanation is always that this will pass, the data are wrong, the other guys are making big mistakes, and if we just make the rear view mirror a little bigger all will see that really everything is fine. Experience suggests this is the reading of a management team that did not live through the difficult days of starting the company, but has instead often risen on the shoulders of others. If the Hyperactive above is in force, the company may be in deal heat, and has often appointed not an operator but a salesman or a lawyer to the top role.

“The best risk management procedures and compliance professionals will not save the day.”
EVALUATING US PROPERLY
WE ARE GOING TO HAVE TO DO
SOMETHING DRASTIC.
SELL, BUY, NEW LEADER, RADICAL
CHANGE IN STRATEGY. IN OTHER WORDS, IF WE ARE NO
LONGER SUCCEEDING, CHANGE THE GOALS. THIS IS OFTEN
JUST ANOTHER VERSION OF DENIAL, AND THIS IS WHERE THE
LEADERSHIP STRUCTURE BECOMES CRITICALLY IMPORTANT.
IS THERE SOMEONE AT THE TOP OF THE COMPANY, THE
BOARD WE HOPE, WHO REALISES THAT CHANGING THE GOALS
WITHOUT ADDRESSING THE SOURCES OF THE DIFFICULTY IS
MOST OFTEN NOTHING MORE THAN REARRANGING THE DECK
CHAIRS ON THE TITANIC? (NOTE THAT THE RANK AND FILE
GENERALLY ALREADY KNOW THIS.) IF SO, CAN THAT PERSON
RIGHT THE SHIP, AS THIS IS WHERE THE END OF THE STORY
IS OFTEN WRITTEN? PRECIOUS TIME IS WASTED HERE, AND
OFTEN THIS STAGE DOES NOT END UNTIL THE COMPANY
LITERALLY RUNS OUT OF CASH.

The Whiner. Should the company still exist at this
point, we will see much handwringing, usually tied to
a corporate myth of some sort: “we are the low cost
producer” is a common one, or “we are the only xxx
in the yyy.” By this time, everyone is yawning, and
the question is how best to use the remaining assets
and cash, when all the options the company once
had seemed to have evaporated, overnight, according
to management.

The Antidote. As stated at the outset, humble
and self aware leaders are necessary but not
sufficient for picking a company’s way through
these minefields to sustained success. And the
best risk management procedures and compliance
professionals will not save the day. The best route
to protecting the company from these treacherous
behaviours is to rely on the vigilance of a board
of directors that brings that precious commodity:
perspective, gained from various deep and broad
experiences outside the worldview of the company
and its leaders. Not all boards can or will do this, but
the best ones will press for honesty and answers,
safeguard against the Deluded, the Ostrich and
the Whiner, and be able to discern the difference
between reality, wishful thinking, avoidance, window
dressing and the various other forms of persiflage,
while at the same time continuing to provide both
needed accountability and support to management.

Deborah Hicks Midanek
President
Solon Group, Inc.
T: +1 (917) 853 3598
E: dhmidanek@solongroup.com
Greed, for lack of a better word, is good.” So said Gordon Gekko, the infamous character in the 1987 movie Wall Street. As we look back over the past few decades, it is interesting to note how fact can mirror fiction. From reading the newspaper or watching the TV news, we know all too well what happens to real-life business leaders who sell themselves out for corporate profits or personal gain.

These ‘sensational’ stories are just the tip of the iceberg. Every day thousands upon thousands of companies are suffering from expensive, time-consuming and energy-draining problems with customers, employees and vendors because of a culture that is based on greed. This may not always get them in trouble with the law, but the risks are nonetheless significant.

On the other hand, a culture that is based on the core values of the organisation contributes to the company’s success. A winning culture is a foundation for attracting and retaining happy, loyal and engaged employees which in turn, attracts and retains happy, loyal customers; both of which are good for business.
Yet, many companies give core values no more than lip service, if they give them any attention at all. Why is that?

Perhaps it’s because many executives have the mistaken notion that core values and profitability are mutually exclusive. This is not true. Honouring core values increases trust, trust increases loyalty, and loyalty is good for business.

Studies show that companies with high levels of customer loyalty typically grow revenues at twice the rate of their competitors. Customer loyalty also increases profit margins. By some estimates, it costs five times as much to attract a new customer as it does to retain an existing one. Companies with low customer turnover have more time and money to serve their current customers and attract new ones.

A company that retains loyal employees builds an experienced, dedicated and productive workforce that can deliver the high level of service necessary to cultivate loyal, satisfied customers. On the other hand, a company with high employee turnover is at a competitive disadvantage because it’s estimated that replacing an employee costs on average one to three times the annual salary of the employee. Even worse, disgruntled or disengaged employees that remain on the payroll can curtail productivity, damage morale and create personnel problems that consume management’s time and energy.

Although a culture based on core values can lead to profitability, cultivating a winning culture can be elusive, especially when the focus of most companies is on profits. When profitability becomes the guiding principle, instead of a laudable goal, risk in every category increases.

Good cultures take intentional effort to cultivate, while toxic cultures are a result of neglect. Just like weeds will flourish in a garden and choke out the plants around them, a toxic company culture flourishes when values, principles and beliefs are not actively identified, defined, shared, institutionalised and honoured.

The following five principles are essential to intentionally creating a winning culture:

**Owning your own values.** Gaining clarity about your personal values is essential to living life with passion and purpose. Clarity about personal values also is important on an organisational level because all organisations are made up of individuals. The degree of success or failure of the organisational unit hinges on whether the values of the individuals are in alignment with those of the organisation. When personal values and organisational values are misaligned, both the individual and the organisation suffer.

**Defining core values.** You must give meaning to your company’s values by creating clear definitions so everyone concerned understands what behaviours they advocate and forbid. When a company has clearly defined its core values, decision making is efficient and straightforward. That doesn’t mean that every decision is easy, but it does mean
that most decisions, even the most difficult ones, are clear.

*Sharing core values.* Any good marketing executive knows that repetition increases impact. The same is true when communicating your company’s most important message: core values. Front-line managers are responsible for communicating core values constantly and consistently so that everyone on their team understands and owns them. But it doesn’t stop there. Successful leaders also model core values. Words unsupported by actions are hollow. Core values must be caught as well as taught; they must be modelled as well as mouthed.

*Institutionalising core values.* You can have the best definitions and the best intentions; but if you don’t integrate them into your company’s operations – if you don’t institutionalise them – they will have little sustained impact. To sustain the required degree of attention, core values should be woven into the fabric of the organisation so that every department operates in alignment with them. Managers or supervisors are responsible for incorporating their company’s core values into their department’s processes so they influence all actions and decisions. If an organisation’s policies, processes, systems and procedures aren’t aligned with its core values, employees will get caught in the crossfire.

*Honoring core values.* You must regard your company’s core values as non-negotiable or they will become inconsequential. Values-centered leaders expect to be held accountable to the company’s core values and they expect accountability from those they lead. Without accountability, day-to-day pressures can easily override an allegiance to core values. Honouring core values is both the easiest and most difficult thing a values-centered leader will be called upon to do. It’s easy because values simplify decision making by clarifying right from wrong. It’s difficult because honouring values demands courage and conviction, when we may naturally gravitate toward convenience and compromise.

Core values are not merely tools for running your business; they are the foundation on which your organisation rests.”
usefulness, you will toss them overboard whenever they seem to be ‘unreasonable’ or ‘impractical’. Disposable core values are not really core values at all. They’re simply policies, and somewhat flexible ones at that. True core values, on the other hand, are beyond compromise. They are so fundamentally a part of your company’s identity that you will not deviate from them – ever.

Living by core values won’t exempt you from economic downturns, troublesome personnel issues, unreasonable customers, or other challenges. In fact, doing so will sometimes expose you to short-term disruptions. But over the long run, adherence to values will allow you to weather these and other storms with calm confidence. You will be more likely to prosper because you will be operating within a solid framework of right priorities.

Although living core values promotes maximum business success – where a definition of business success includes profitability – we have observed that organisations that benefit most from living their core values tend to define success in light of their values. They’re working for rewards that are substantially greater than profitability alone.

We encourage you to find out for yourself how valuable creating a company culture based on core values can be. Your company will be more prosperous in tangible terms. But even more important, you will grow to appreciate that the greatest value of core values is ultimately in the values themselves. **RC**

**Lisa Huetteeman**  
Managing Partner  
Black Diamond Associates  
T: +1 (813) 785 9768  
E: lisa@the-black-diamond.com
 MANY organisations do not understand the link between strategic risk and strategy. Some simply describe risk as being about enterprise risk management, but this ignores the basic tenet of risk management – that it is about taking opportunities.

Strategic risk underpins all strategy and supports strategic decision making. Why is this so difficult to understand? Probably because people do not readily link strategy with risk. More organisations now understand that unless there is a well formed risk appetite then they are more likely to fail because there is a disconnect between the opportunity and an understanding of strategic risk.

Strategic risk is informed by hindsight, insight and foresight. Strategic risk decisions are also informed by the organisational capacity, strategic agility, the organisation’s business idea, having a competitive advantage, being able to do what you say and in some cases being able to disrupt the market.

Hindsight risk is an important tool in strategic risk. This enables decision makers and boards to understand where the organisation has come from and what it is capable of. It also ensures that those making strategic decisions actually understand the organisation’s capacity to execute strategy. It enables decision makers to be sure that if they are making strategic risk decisions the organisation can support them. If the organisation cannot initially
support the decision then this will also be part of the strategic risk decision making process. This means that if change is required then the strategic risk conversation will include the need for such change.

Insight risk is the second part of this strategic risk process. This involves strategic thinking and applying insight to strategic risk decision making. This means that the decision makers build on the hindsight process and apply their insight to the market, the risks and whether this is the right strategic risk decision to make. Insight is difficult to quantify but it is often characterised as intuition and consideration of the risk appetite of the individual and the overall risk appetite of a board or executive management team. It can be the ‘gut feeling’ that this is a right or wrong strategic decision.

Foresight risk is about taking the organisation, say, one, three, 10 or more years into the future. The aim is to look into the future at the barriers to success and failure, and balance these with the amount of strategic risk the organisation should be taking. This type of strategic risk based planning is not an exact science. In fact it builds on the hindsight, insight and foresight to form a view. Obviously, you will never get this exactly correct. The important issue is that the board and management take themselves into the future to understand the opportunities and barriers to success and failure.

In combining these three concepts it is important to understand what success and failure look like. This is a key determinant in any strategic risk process.
Too often we look at success indicators when we should also be looking at the early warning signs that we are failing. In considering the strategic risk foresight process it is important to have a robust discussion about what exactly success looks like and how you measure it, and in turn what failure looks like and how you measure it.

Some people say that you should avoid the word failure in discussing strategic risk. Why? If you simply think you will succeed then you are going to be surprised when you fail. You may want to use another descriptor other than failure. In the end you need to agree that whatever word you use when you stop succeeding and start failing, it is best to know earlier rather than later.

Nearly all of the best strategic risk failures involve people who do not think they can fail. In most of the reports written by this author and the majority of reports on major failures the following strategic risk issues emerge:

*Group think*. The group thinks everything is fine and avoids completion and/or the hard decisions. This represents a lack of perception around the hindsight, insight and foresight risk issues. Rather than using a strategic risk approach, they assume nothing can go wrong and do not stop to consider the potential to fail.

*Lack of defences in depth*. Understanding that multi-layered organisational processes and behavioural defences are essential to reduce the opportunities for failure. This is the second strategic risk failure. If the decision makers do not consider the strategic risks and do not look at the type of defences in depth, then they will fail. If you have too many defences, nothing will happen but if you do not have enough, you will look foolish.

“In considering the strategic risk foresight process it is important to have a robust discussion about what exactly success looks like and how you measure it, and in turn what failure looks like and how you measure it.”

*Confirmation bias*. The group confirms a particular bias without stopping to ask why – this is often a failure that occurs in strategic risk. People think that they are making independent decisions when they are merely confirming their existing biases. This reflects a failure to consider hindsight, insight and foresight in decision making. Often it is an assumption that all will be well when it is not. This represents both a behavioural and procedural risk.
process that often informs bad strategic risk decision making.

_Tunnel vision management._ Where the management and the board can only see what they want to see. This is another of the failures in strategic risk. People feel comfortable with what they know and do not bother to ask the ‘what if’ question. If you do not ask the ‘what if’ question then you do not recognise your capacity to fail and you will be surprised when you do fail. This type of decision making is a common element in the failure of strategic risk decisions and is common in most of the major enquiries into large corporate failures, corruption, rail accidents, oil fires, plane crashes and similar events that organisations do not expect to occur.

Another element to strategic risk decision making includes strategic agility. This means that, in understanding how to make strategic decisions, the organisation needs to understand its agility. In a start-up enterprise this strategic agility is likely to be more adaptable than in a large company. Nevertheless, the capacity to apply strategic agility to strategic risk is critical. If you cannot respond quickly, decisions regarding strategic risk will need to be undertaken over a longer period of time. Regardless of how this occurs, creating reports that are easy to understand will show that this agility is being applied.

Other worthwhile considerations in strategic risk are: does the organisation have a business idea? Is this well thought out and does anyone across the business understand it? This often gives you a competitive advantage in a market. Strategic risk is generally informed by this competitive advantage. On the other hand, it is also possible to create a competitive advantage by disrupting the market with a new idea or product. The idea of disrupting the market is best illustrated by the mobile phone, which on any definition has disrupted the market. From a strategic risk perspective, those of us who were alive in the 1980s could not have accepted that a portable mobile phone would have changed the world as it has. Often in strategic risk, disrupting the market will start slowly and then grow over time. In that case a good idea should not be left behind because it is different.

Once you have worked your way through these issues it is time to look at the strategic risk cycle. The application of this decision making model is important in understanding and applying strategic risk.

In applying this model it is important to ensure that the board (and other senior executives or senior government officials) understands the difference between enterprise risk and strategic risk. Enterprise risk is a consequence of the strategic risk decisions made by the board or leadership team.

In the first instance the board needs to understand its role in strategic risk. It needs to establish a risk appetite and set performance and conformance
reporting arrangements to assure that this risk appetite is in place across the organisation.

At all stages of the process there must be an informed link to the mission, vision, values and culture of the organisation. If this alignment is not made then the process of strategic risk management will only manage procedures. These situations generally lead to failure because there is no alignment between the strategic risk and behaviours and culture.

The board then needs to undertake strategic thinking which will inform the management on how to prepare the strategy for the board’s approval based on the strategic risk model above.

If there is a disconnect in strategic risk because of changed circumstances, the organisation should stop and start again.

In the end, strategic risk is a critical part of any organisation’s operations. Understanding the opportunities this creates is important and recognising the potential to fail and succeed is critical. **RC**

---

**Neill Buck**
Consultant
Neill Buck & Associates
T: +61 2 9235 0070
E: nbuck@comply.com.au
The value proposition of Enterprise Risk Management (ERM) seems in many ways compelling. ERM seeks to build upon traditional risk management practices that are conducted within functional or programmatic siloes, and engage in the cross silo conversations and prioritisations needed to develop an enterprise-level, portfolio view of risk. The ultimate goal is improved return on investment in meeting overall stakeholder needs. Why would any organisation not strive to achieve such an integrated view of organisational risk?

Yet despite the inherent appeal of ERM, the allure and the reality are different for many organisations. Organisations are finding that what seems on the surface like such an obvious step forward is in fact a long-term commitment that requires both planning and resources. What is the difference between an organisation that establishes a vision for ERM and makes methodical progress towards that goal, and an organisation that seems to flounder and face more than its share of detours? Answering this question requires considering what makes any major initiative more challenging than often envisioned, and how such general challenges apply to ERM in particular.
Numerous studies over the past two decades, beginning with that of organisational change guru John Kotter, have shown that only 30 percent of change programs are considered fully successful. That poor level of success has remained relatively consistent as evidenced by repeated studies over more than 20 years. Mr Kotter’s research and that of numerous studies since have pointed to the inadequate attention provided to organisational change management. In this context, we are not referring to the changes in policies, procedures and various actions reflected in a project plan. Most initiatives pay considerable attention to the physical changes that must take place to implement any organisational change initiative. What is frequently lacking, however, is an equal focus on the requisite behavioural changes – both at the organisational and individual levels – that must take place. These behavioural changes are essential to: (i) successful implementation of any major change initiative; and (ii) the sustainment of the change needed to avoid reverting to old behaviours.

Considering the organisational change management aspects of ERM is important because successful implementation of ERM requires more than new policies and procedures. ERM requires new ways of behaving, both in how risks are viewed relative to other stakeholders in the organisation and how risks are balanced with consideration of performance and cost. Too often ERM is viewed as simply ‘mature’ risk management where policies are honed and practices are consistently followed. Such a simplistic view overlooks significant behavioural changes that are typically required for the implementation of a meaningful ERM program.

To appreciate the behavioural changes required for ERM, it is useful to consider typical practices in traditional risk management. Effective risk management should be an element of every business decision in which benefits, costs and risks are interactively balanced with the goal of maximising overall long term stakeholder value. Too many organisations, however, focus such a balance on costs and benefits, and treat risk as simply a gate through which decisions otherwise made must pass. In other words, the approach of these managers is to make the cost-benefit tradeoff and go forward unless the associated risks are too great. Treating risk not as a function of a risk management organisation, but as an inherent part of every business decision, is a new way of thinking – and behaving – for many individuals.
A second major behavioural change required by ERM is recognition that those impacted by risks are not limited to those whose technical expertise is core to understanding and controlling the risk. For example, while understanding and managing IT risks may require the hands-on engagement of the IT staff, those impacted by a breach in IT security can truly be enterprise-wide. In the IT breach of Target stores, for example, the impact had major consequences across much of the organisation, resulting in lawsuits, the removal of the CEO, and numerous other adverse consequences. Setting risk appetite, and ensuring actions taken lead to managing risk within that appetite, clearly cannot be limited to the IT staff. Traditional risk management tends to identify, assess, and treat risks within their respective functional and programmatic siloes. ERM, however, recognises that key risks be communicated and prioritised across the overall enterprise. In this way, those impacted by residual risk have a voice in the adequacy of the risk treatment. Moreover, only through ERM can a truly enterprise-level portfolio view of risk be developed. Such a portfolio view of risk is essential to understanding the organisation’s overall level of retained risk, and consistency of that risk with the organisation’s risk appetite and capacity for risk.

Because of the more collaborative approach to risk management required by ERM, many individuals may have to change their attitudes in working with others on the topic of risk. Engaging in cross-functional risk workshops will be a new experience for some individuals, who previously
only coordinated within their functional silos. Having to defend risk treatment choices based on residual risk felt beyond the functional silo, and having to defend return on investment from risk treatment versus use of those funds to treat risks in other functional areas, may both be new experiences. While the list of changes resulting from ERM can go on, the message is simple. ERM will require individuals to develop new working relationships and engage in new responsibilities. In short, behaviour will have to change. While such a conclusion may be relatively easy to reach, effecting the necessary behavioural change can be challenging, as reflected in the previously cited studies. Recognising the importance of a formal organisational change management program as part of any such major initiative is certainly a starting point.

Even when ‘organisational change management’ is included as part of a major initiative, for too many leaders that term simply means the inclusion of a communications plan to communicate the coming change, and a training plan to train employees in the new processes. Nearly two decades ago this author created a change management model intended to convey the larger role of effective change management, referred to as UMTI. This model was based on the following:

**Understanding.** Individuals and organisations need to understand the importance and reasoning behind a change initiative. This is winning the ‘mind’ of the individual through intellectual awareness and understanding.

**Motivation.** Once individuals understand the reasons for change, they must be motivated to act on this change. There are many reasons why individuals may choose not to support a change even when they understand the rationale behind the change. This step wins the ‘hearts’ of those whose support is needed.

**Tools.** When individuals understand the need for change and are willing to engage, they still need the capacity in terms of knowledge and ability. ‘Tools’ was intended to reference the policies, procedures, processes and technologies required for an understanding and motivated individual to act.

**Incentives.** It is difficult, if not impossible, to sustain new behaviours when old behaviours continue

“ERM will require individuals to develop new working relationships and engage in new responsibilities. In short, behaviour will have to change.”
to be rewarded. ‘Incentives’ refers to rewarding the desired new behaviour and discouraging the old behaviours used prior to the change. New performance standards must be developed and connected to appraisal systems to ensure that changes are sustained and guide future actions.

In 2006, Jeff Hiatt authored the book ‘ADKAR: A Model for Change in Business, Government and our Community’. In his book, Mr Hiatt proposed a compatible model of Awareness, Desire, Knowledge, Ability and Reinforcement. While Hiatt chose different words to represent similar concepts, and chose to separate Knowledge and Ability (referred to as ‘tools’ in the UMTI model), the ideas are essentially the same: all elements of the UMTI or ADKAR models are essential for sustainable individual change. The ADKAR model has since gained broad international recognition as an effective description of the key phases in individual change.

Finally, organisations seeking to implement ERM should consider the needs of a successful ERM program implementation versus the capacity of the overall organisation to support required change. Because all initiatives present unique requirements for success, and all organisations have unique capacities for change, change leaders should consider where gaps exist between specific needs and capabilities. Resources must then be targeted on closing the most critical gaps. The 2009 book ‘Chasing Change: Building Organisational Capacity in a Turbulent Environment’ provided an assessment tool to size these gaps between initiative requirements and organisational capacities for change. This book considered various elements of successful change (leadership, commitment, accountability, forward thinking, communication, risk tolerance, and others), and provided a maturity model for sizing the gap in these elements as related to a specific change initiative. Whether using such tools, or otherwise considering the hurdles to successful change, ERM champions will be far more successful in their efforts when they consider and overcome the various individual and organisational impediments to sustainable change. RC

Dr Doug Webster
President
Cambio Consulting Group
T: +1 (703) 441 2212
E: dougwebster@cambiocg.com
The debate over board oversight of risk management continues. And the central issue is the same. How is risk most effectively overseen by the board of directors? Should there be a board-level ‘risk committee’? Should risk oversight be spread among a number of committees? Should risk management oversight reside with the full board?

Some board members are dead set against a separate risk committee. They point out that risk oversight is a full board responsibility. And they observe that risk is inseparable from strategy and that a board-level risk committee might operate to unduly constrain those able to participate in key discussions.

Others argue that a board-level risk committee is critical. They point to perceived risk management failures during the financial crisis and the particular expertise needed to interact with the risk management professionals. They also contend that some sort of board-level risk committee needs to exist, if for no other reason so that there is some place for enterprise risk management to go.

Audit committees have a lot of skin in this game. In the absence of a board-level risk committee, audit committees can find themselves with responsibility
for oversight of all sorts of risks. They may include credit risk, liquidity risk, operational risk, cyber security, environmental risk and ‘overall legal compliance’. That is a lot to ask of a committee whose expertise resides in financial statement presentation and disclosure.

But the problem is not just one of expertise. Another problem is time. As audit committees get drawn further and further into collateral areas of risk management, they stand to be increasingly distracted from their core responsibility: financial reporting. Sarbanes-Oxley places squarely within a US audit committee responsibility for the oversight of financial reporting. And the statute contains no exception for audit committees that are too busy with other things.

Nor does the US SEC appear to be in a particularly forgiving mood. The SEC recently brought charges against an audit committee chair who, as the SEC perceived it, was not properly fulfilling his financial reporting ‘gatekeeper’ function. At the same time, the SEC’s chief accountant has been encouraging audit committees to get ‘back to basics’. A particular peeve of the SEC is audit committees too busy or distracted to pay enough attention to the audit fee and delegating that task to management.

How did audit committees get into this fix? Recent history helps explain. In the wake of a number of high-profile financial reporting failures, audit committees were often perceived to be the most independent and active of the board’s committees. As the need for additional board oversight increased, the logical place to put the responsibility seemed to be the audit committee. That is certainly how the New York Stock Exchange (NYSE) seemed to approach it. The NYSE wrote rules taking the audit committees of listed companies well beyond the

“How did audit committees get into this fix? Recent history helps explain. In the wake of a number of high-profile financial reporting failures, audit committees were often perceived to be the most independent and active of the board’s committees. As the need for additional board oversight increased, the logical place to put the responsibility seemed to be the audit committee. That is certainly how the New York Stock Exchange (NYSE) seemed to approach it. The NYSE wrote rules taking the audit committees of listed companies well beyond the

“Some board members are dead set against a separate risk committee. They point out that risk oversight is a full board responsibility.”

boundaries of financial reporting into, essentially, all risks a company may face.

But now, some audit committee advocates are pushing back. One audit committee adviser has cautioned that audit committees in substance have become the ‘default committee’ – the committee that gets responsibilities that don’t seem to fit
anywhere else. A committee of the New York City Bar Association recently wrote to the NYSE urging revision of the NYSE rule mandating broad audit committee risk oversight. An international group, the Society of Corporate Secretaries & Governance Professionals, has been agitating with increasing vigour for change.

What’s an audit committee to do? The first thing is to recognise there simply may not be a one-size-fits-all solution. For some boards, a separate risk committee may make sense; for others, not. But the key thing is for an audit committee to ensure that it has the time and resources to fulfill its legally mandated financial reporting responsibility. If it does not, that is not just a problem for the audit committee. The entire board has an interest in seeing that the audit committee gets it right.

And if the audit committee is too busy? One possibility would be to look at the risks given to an overly burdened audit committee and divide them into two groups. One group, quite obviously, would be those risks associated with financial reporting. The second group might be thought of as ‘other’.

As to the first group, those risks should obviously stay with the audit committee. As to the second, if they are to be placed within a committee, another committee or committees need be found. In the absence of anything better, perhaps the second committee should be called the ‘risk committee’. RC

Michael R. Young
Partner
Willkie Farr & Gallagher LLP
T: +1 (212) 728 8280
E: myoung@willkie.com
When it comes to questions of ethics, values and risk management, boards often experience the same dangers that other groups do: the danger of group-think and the inability – or perceived inability – to speak up safely and constructively without fear of ostracism or retaliation. If board members are unable or unwilling to address difficult matters, the dangers to the organisation are clear, especially in light of the fact that the buck for risk oversight stops at the board. We’ll never know how many serious concerns or even scandals might have been stopped or curtailed if not for the pervasiveness of such group-think or reluctance to speak up within a board.

Using a hypothetical scenario of an all too familiar case about how to handle sensitive information within the corporate boardroom, we demonstrate how the ‘Giving Voice to Values’ (GvV) methodology for values-driven leadership development can be useful even at the highest echelons of an organisation, and provide directors and boards with a toolkit to approach such difficult and critical internal communications more successfully. This ultimately is a form of governance best practice and risk management at the highest levels of an organisation.
Hypothetical scenario

The audit committee chair of company XYZ, Mr Jack Jones, receives a verbal report from an internal audit (IA) director, Ms Carol Cooper, that the head of human resources (HR), Ms Greta Major, has been pressuring her staff not to fully cooperate with IA. It is not clear whether this is a simple jurisdictional dispute between IA and HR or something more serious.

Mr Jones speaks privately with the CEO and Chairman, Mr Peter Pan, who assures Mr Jones that Ms Major and the head of IA, Mr Mark Minor, have a difficult working relationship based purely on personality. Mr Pan assures Mr Jones that these are just turf battles and that he is ‘on it’ from a performance management standpoint.

Separately, Mr Sam Smith, another board member, has an informal conversation with a member of the IA team during a meet-and-greet lunch between board members and XYZ staff. The IA staffer, Mr Manny Minnow, tells Mr Smith that the reports of functional turf wars between HR and IA, while true, are obscuring legitimate complaints by HR personnel that they are being pressured to downplay or withhold information from IA. Mr Minnow says that he has serious concerns about the leadership style and workplace tactics of Ms Major. Mr Smith makes a point of sharing this information with Mr Jones.

On the day of the XYZ board meeting, the only board members, other than the CEO, who have heard about these problems, are Mr Jones and Mr Smith, who are both present at the full board meeting. The board meeting proceeds according to its agenda, which includes an executive session, without anyone raising the IA/HR issues. While Mr Smith is concerned about what he has heard, he also does not want to damage the reputations of key executives or suggest that he does not trust Mr Jones’ or the CEO’s ability to handle the situation.

Analysis

If this were a traditional scenario, the concluding question would be: Should Mr Smith raise this issue? The discussion would be about the pros and cons for speaking up and their consequences.

Some might argue that Mr Smith should say nothing and do nothing. After all, this is not really
Mr Smith’s responsibility as he is not on the audit committee.

Others might suggest that he may do more harm than good, triggering an investigation into something that others (the CEO and Mr Jones), who are closer to the key players, have concluded is a non-event. Expense would be involved; suspicions would be raised; relationships would be damaged. After all, doesn’t Mr Smith trust his fellow board members and the CEO to do their jobs effectively?

Others might note that there is no evidence other than that of personality clashes.

Finally, it is quite possible that the complaints Mr Smith heard are a staffer’s disgruntled complaints against Ms Major.

**GVV analysis**

Applying the GVV lens to these issues, however, we would ask an entirely different question. Rather than asking whether Mr Smith should act and speak, GVV encourages us to consider how he could do so effectively. GVV is about shifting the discussion of values-driven leadership away from an intellectual debate about what is ‘right’ to a more pragmatic emphasis on effective values-driven decisions.

When it comes to ethical questions, we often de-skill ourselves, shifting into a simplistic view that ethics are all about ‘speaking truth to power’.

GVV’s shift from ‘analysis’ to ‘action’ unleashes the same innovative thinking and strategic acumen that executives and board members typically apply to other business challenges.

What this means for Mr Smith is that, assuming he wants the right outcome, instead of asking “should he raise the issue at all?”, we would ask how can he do so most effectively. The following core GVV ‘scripting’ questions would be asked:

*What is the values-based position that Mr Smith wants to address?* This is an important question because resolution of this issue can go wrong if attention is focused on personalities rather than the goal of ensuring comprehensive and efficient audit processes, for example.

*What is at stake or at risk for all affected parties, including Mr Smith himself?* The point isn’t to try to balance the risks to all, but to understand what might be motivating – or de-motivating – key players.

“When it comes to ethical questions, we often de-skill ourselves, shifting into a simplistic view that ethics are all about ‘speaking truth to power’.”
so that Mr Smith has more ways to frame his queries. If he learns that the CEO has encountered previous difficulties in managing Mr Minor and Ms Major’s interactions and is therefore loathe to stir up the hornet’s nest again, Mr Smith can suggest a process that is attributed to the board instead.

What are the ‘reasons and rationalisations’ Mr Smith is likely to encounter? Mr Smith has the chance to literally pre-script and rehearse his responses to the predictable objections he could encounter. There are four common ‘reasons and rationalisations’ in business: (i) it’s standard operating procedure; (ii) it’s not material; (iii) it’s not my responsibility; and (iv) it’s a matter of loyalty. Several of these were generated for Mr Smith in the above analysis. These rationalisations are common, predictable and vulnerable to response if we have the chance to pre-script and rehearse.

What is the most effective action plan and script for making sure that this issue is properly addressed? The goal is to generate not just one approach but several, so that Mr Smith has options and is more likely to be effective. Depending on his answers to the questions above, Mr Smith may conclude that he should work through quiet channels, like the Chief Ethics and Compliance Officer. Or he may decide to bring the issue to Mr Jones’ attention one-on-one. Or he may conclude that both the CEO and Mr Jones are not taking the issue seriously and that he needs to raise the question with the full board.

The GVV approach is based on the idea of rehearsal and pre-scripting to create a sort of ‘moral muscle memory’ or ‘default to voice’, albeit an informed voice: a considered strategic approach to enacting values-driven leadership. Ethical leadership is not just about making decisions, nor even just about speaking up, it requires voicing one’s own values effectively to senior peers; creating a culture that encourages and accepts such voice; and building the capacity to listen to the voices of others. True ethical leadership carries an expectation of efficacy and skill — doing the right thing is not just a matter of analysis. If we want true ethical leadership, we need to focus on action.

RC

Andrea Bonime-Blanc
CEO and Founder
GEC Risk Advisory LLC
T: +1 (917) 848 4448
E: abonimeblanc@gecrisk.com

Mary C. Gentile
Director, Giving Voice To Values
Babson College
T: +1 (781) 648 3220
E: mgentile3@babson.edu
THE LACK OF STRATEGIC INFORMATION CAN LEAVE MONEY ON THE TABLE

BY GARY W. PATTERSON
> FISCALDOCTOR

The information package that the board receives is critical to the fulfilment of its governance responsibilities. Yet it is too common a practice for board members to be given reports only a few days before the meeting, greeted with hastily prepared bits and pieces of additional information as they walk in the door, or treated to mind-numbing PowerPoint presentations about organisational minutia.

There is a better way which begins with first asking the question: “What information does the board need to do its job?” We recommend that management provide board members with one-page financial and operational summaries that are written at the strategic level which reflects the board’s proper role and where it can add value. Making this happen means assigning resources to providing the information they need, putting processes in place and often overcoming a number of significant challenges.

There are a number of common obstacles. Accounting systems may be inefficient or inadequate for collecting timely and critical financial data. Sometimes accounting departments due to lack of resources or unwieldy software just don’t have the capacity to prepare, analyse and distribute the financials in time for a board meeting. Further, information across departments is not easy to capture. A strategic information package for board members requires that departments such
as marketing, sales and IT work collaboratively to collect, analyse and interpret financial and operational data. Finally, the company may lack the capacity to prepare for board meetings. The reality for some companies, especially those in high growth mode, is that they don’t have the time, infrastructure and people to put together an information package that is geared to the strategic needs of board members.

The best approach is to have the organisational initiative for the provision of timely financial and operational information come from the board itself.

Although it may require some strengthening, the functional role of board secretary is the ideal role to assure that board members receive quality information well in advance of meetings. If the board doesn’t have a designated board secretary, it should consider adding this capability even on only a part-time or outsourced basis. This person will be the board’s spokesperson and liaison to management so she must be able to effectively represent the board’s interests and work with C-level executives.

The practical options for filling this part time function are additional internal accounting staff or outsourcing to a CPA firm or another financial consulting firm. The key determinant is the requirement for a quality end product which is to offer timely strategic financial and operational information supporting the board’s governance role.

Whatever resource is given the task, she must have the deep experience and strategic vision to meet the challenge. Some pertinent questions regarding this part time function are: Can we restructure a position within the internal accounting or financial organisation to fulfil this corporate secretary function? Is the management culture of the firm such that an employee would be given the autonomy and independence that the corporate secretary role requires? Does your CPA have commensurate level of expertise and respect to drive the information package reporting process? Is there another financial consulting firm that can meet the requirements for the board’s corporate secretary?

Whoever is chosen to fill the corporate secretary role will have to work through a number of key steps to enable the organisation to deliver a quality information package to its board of directors.

**Step One:** Break the data logjam. The board secretary should work in concert with the CEO to make a quality information package a management priority. She should work with both CEO and CFO to establish a process to accelerate the system for collecting data for the board package. Both management and the board need to agree on the timeframe in which this data needs to be collected in advance of board meetings.

**Step Two:** Investigate who worked the logjam issue in the past. We have often found that whenever management and boards begin to examine this issue, individual groups such as sales, marketing or technology attempted to address the problem...
and provided solutions but management found the information to be too functionally oriented or “it wasn’t the right time” to implement the reporting package. The corporate secretary can talk to the ‘historian’ of the prior effort and provide the board insight into why it was not successful. This history can give context to a discussion with the CEO about how to refine the means of data collection or the creation of a new strategy. This proactive approach to facilitate the flow of information to the board will empower the corporate secretary to see that critical information is presented to the board and ensure that the board has the tools to make informed decisions.

*Step Three*: Streamline data collection, analysis and distribution. It may be difficult to obtain and analyse information in a timely manner. Under these circumstances, the corporate secretary should advise the CEO to consider the following recommendations: (i) speed up the financial statement’s closing timetables; (ii) improve the operating or financial reporting system; and (iii) eliminate some existing reports altogether.

*Step Four*: Keep the board package simple. One-page financial and operational summaries at the strategic level will facilitate the high level discussions in the boardroom necessary to chart the company’s long term future.

The benefits of providing a timely information package are threefold. Firstly, directors are positioned to offer insightful, well-thought out recommendations if they get the materials early having time to review and think about the issues that are on the table. The board’s focus on strategic issues is the best use of their time and where they can add value to the overall enterprise. Secondly, the CEO and board members receive the gift of time to reflect and collaborate on the key strategic issues that will help the company grow and prosper. Finally, effective internal control over financial reporting and information security is a requirement of good governance which can be fulfilled by careful distribution of the information package.

The quality of a board’s decisions reflects the quality of the information that they have in hand and the time that they are given to do the work of making strategic decisions. The corporate secretary’s role is the lynchpin for developing and implementing the process to deliver clear strategic information to the board in a timely fashion. It is the responsibility of management to use their boards effectively because the company ultimately must bear the consequences of a board’s strategic decisions.

---

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

---
MITIGATING REPUTATION RISK FOR SUCCESS: STRATEGIC PLANNING IN TODAY’S MULTI-STAKEHOLDER, MULTI-CHANNEL ENVIRONMENT

BY JOHN PATTERSON
> REPUTATION INSTITUTE

Reputation risk management emerged as one of the most dynamic areas of business strategy during the first decade of the 21st century and hasn’t showed any signs of slowing down in the aftermath of the 2008-2009 global financial crisis. Consider these four data points:

First, the number of publications containing reputation risk in their title or abstract has more than doubled since the year 2000, according to the Conference Board.

Second, in 1990 there were only two mentions of reputation risk in the global media (this in the immediate aftermath of the Exxon Valdez oil spill), compared with 270 in 2006 and more than 1000 in 2012, according to Weber Shandwick.

Third, today 75 percent of risk managers from
in institutional investors believe that risk was given the highest priority after the financial crisis of 2008-2009, according to The Economist.

Finally, besides financial risk, reputation risk has emerged as the most important area of risk management to boards of four different kinds of companies: 66 percent of public companies, 70 percent of private companies, 77 percent of not for-profits and 65 percent of private equity-owned companies, according to EisnerAmper.

Leading companies are now beginning to see the business value in connecting the dots between their corporate reputation strategy (ensuring there is a clear road map for how to make progress on reputation priorities, the resources required and who will be responsible) and planning and simulation (developing tools and processes that help ensure cross-stakeholder expectations are being used as a core criteria in developing and testing business plan priorities, and specific programs and initiatives). A key success factor is making sure reputation risk – not just opportunity – is factored into the equation.

The fundamental question in looking at reputation risk beyond just being a ‘risk of risks’ comes down to this: how does one establish impact and likelihood of a risk from a reputation perspective? The risk impact is assessed by the areas of importance (23-30 individual attributes underneath the seven rational dimensions of reputation – Products & Services, Innovation, Workplace, Governance, Citizenship, Leadership and Financial Performance) to external stakeholders that provide the degree of impact that each risk will have on corporate reputation. The risk likelihood is the difference, or gap, between external perceptions, and internal perspectives (or reality) indicates how likely a risk is to materialise.

In discussions with
reputation champions from Western multinationals like BP, Carnival and Sprint, as well as emerging market leaders including Itau (Brazil), MTS (Russia) and Eskom (South Africa), we see four open implications for reputation risk that must be addressed before the organisation can credibly claim that it is ready to integrate reputation risk management into the annual business planning cycle: (i) awareness of reputation risk, but not understanding; (ii) reputation risk is difficult to evaluate and quantify and still lacking a standard; (iii) reputation risk management primarily lies with the CEO, but it is unclear who runs with it; and (iv) risk culture is embedded, but it is not embedded: what does it take to embed risk in company culture?

Once the open implications have been resolved, the reputation champion (usually a senior communicator or occasionally the CMO) is ready to address four key intersection points between strategic planning and reputation risk management:

Cross-functional internal collaboration. This is often a mixture of collaboration and relevance (collaborating with businesses and functions to ensure the corporate reputation strategy is relevant to their needs and enables them to do their jobs better in the event of a negative reputational event) and cross-functional management (managing corporate reputation across businesses and functions, based on clear priorities, responsibilities, and Key Performance Indicators). Leading organisations such as Johnson & Johnson, FedEx and Novo Nordisk have actively managed their corporate reputation through challenging times and events in part because their planning processes are both operational (risk assessment over multiple years impacts the strategy) and inspirational (leaning on legacy and heritage to build equity and resiliency) at the same time.

Mergers & acquisitions. Combining two organisations with vastly different reputation risk profiles is often the most difficult part of M&A due diligence and post-merger integration. Classic examples include BP/Amoco (1999), HP/Compaq (2001) and Sprint/Nextel (2005), but two more recent examples from the banking industry of Toronto-
Dominion Bank/Commerce Bancorp (2007) and Itau/Unibanco (2009) proves that it can be done successfully.

*Industry reputation risk.* Every company’s licence to operate relies heavily on both social and political will to allow its industry to compete more on differentiation and less on compliance. When an event like 9/11 occurs for the travel and tourism industry or the 2008-09 financial crisis and Occupy Wall Street movement for the financial services industry, it changes the rules of engagement and the realm of what is possible in the short run for all industry participants. Those organisations with a strong reputation who are able to separate themselves from the pack during these difficult times (think USAA as the only financial services company in the US to be exempt from the Volcker Rule/Dodd-Frank legislation) in part because multiple stakeholders believe that their reputation inoculates them from the trust deficit that infects the rest of their peer group. However, examples like USAA are the exception and not the rule. But other organisations, like Southwest Airlines in the wake of 9/11 and BlackRock in the aftermath of the financial crisis, were able to define the future of industry competition on their terms, not the regulators’.

This led to permanent market share and mindshare increases for these one-time underdogs, at least in part because they were better able to assess reputation risk than the usual suspects and avoid the pack behaviour of their industries.

*The road to recovery post-crisis.* It is critical to have sustainable ambassadorship or advocacy in place before a reputational event occurs – the best companies enable supporters to be ambassadors for the company, its products or services, and relevant societal concerns related to its core business. This doesn’t happen by accident – good strategic plans are built around employee alignment, not merely engagement. In addition, transformational investments (ensuring the company is making transformational changes in the way it does business to deliver on what it stands for) are crucial for the company to be able to turn the page.

In conclusion, linking a firm’s risk register to reputation risk analysis in order to map and classify by impact and likelihood is one way to ensure that the strategic planning process will allow reputation risks to be clustered to inform mitigation strategies before a negative reputation event occurs. In today’s commoditised and globally competitive marketplace, where no one is in charge and everyone has a voice, mitigating reputation risk for success is no longer optional.

---

**John Patterson**
Senior Advisor
Reputation Institute
T: + 1 (212) 495 3855
E: jpatterson@reputationinstitute.com
WEATHERING THE STORM: COMPANIES WILL NEED TO TAKE STEPS TO ASSESS AND MANAGE CLIMATE RISKS

BY JANET PEACE 
> CENTER FOR CLIMATE AND ENERGY SOLUTIONS

Companies have always had to navigate a changing business environment. But now they face a changing physical environment, as climate change contributes to more frequent and intense heat waves, higher sea levels and more severe droughts, wildfires and downpours.

Businesses are increasingly recognising that these climate impacts are imposing real costs, here and now, in the form of damaged facilities, interrupted power and water supplies, higher insurance costs, and disrupted supply and distribution chains.

Despite the growing awareness, many businesses continue to plan using a historical picture of risks – an inaccurate picture that fails to take into account how climate change is rewriting the future. A major reason is that data about climate risks and potential damages are difficult to obtain at a scale useful for business planning. Two steps toward addressing
this need in the United States are President Barack Obama’s new Climate Data Initiative and the newly released National Climate Assessment.

**Recognising the impacts**

According to Munich Re, about 800 major weather-related disasters worldwide in 2012 led to more than $130bn in losses, with the most costly events (Hurricane Sandy and the Midwest drought) occurring in the United States. Last year, we saw costly flooding in central Europe, a deadly typhoon in the Philippines and a crippling drought in California. These events serve as reminders of our vulnerability to extreme weather, which climate change will exacerbate.

Ninety percent of S&P Global 100 Index companies identify extreme weather and climate change as current or future business risks, according to a recent report by the Center for Climate and Energy Solutions (C2ES). More than 60 percent said they are experiencing climate impacts now, or expect to in the coming decade.

Companies are concerned about direct impacts, such as extreme weather damaging facilities or closing their doors, and also indirect impacts, such as higher prices for commodities or insurance. Companies also worry about risks they can’t directly manage – those outside their ‘fence line’ that can still affect the bottom line. For example, extreme weather can keep employees from getting to work, disrupt transportation and communication systems
and threaten the availability of energy, water or raw materials.

Hurricane Sandy in 2012 illustrates this fence line issue. About 75 percent of small businesses hit by Sandy had to close their doors for a period of time, many for at least a week, according to a survey of 450 businesses by The Hartford insurance company. But the major challenge wasn’t damage to buildings; it was a loss of connection to the grid. Only 11 percent of businesses reported structural damage, while 71 percent experienced a power outage, showing the importance of thinking beyond the fence line when assessing climate risks.

Companies are also learning first-hand that even when their own risk assessments take climate change into account, their operations can still be disrupted if their suppliers have not taken the same steps. For example, a single event — extensive flooding in Thailand in 2011 — badly damaged global suppliers of parts for the automotive and electronic industries, hurting the bottom lines of Ford, Honda, Toyota, Dell, Cisco and many other companies. Direct losses from the floods were estimated at $15-$20bn.

**The four-step process**

While the vast majority of major companies acknowledge the risks from extreme weather and climate change, most are using existing business continuity and emergency management plans to manage these risks. Companies going beyond ‘business as usual’ generally depend on a key commodity, operate in high-risk locations such as a low-lying coastal area, or see a clear business case for action, such as opportunities to become more efficient, reduce costs or provide greater value to customers. Generally speaking, these leading companies follow a four-step process.

“Companies are also learning first-hand that even when their own risk assessments take climate change into account, their operations can still be disrupted if their suppliers have not taken the same steps.”

Step one is to build a common understanding across the company of the risks associated with extreme weather and climate change – based not only on the past but on what could change in the future. For example, the mining giant Rio Tinto has brought in external partners to brief senior executives on climate science and the business implications of climate change. The company is starting to consider climate risks in water management and the engineering of new projects.
The next step is risk assessment: determining how changes in the likelihood or magnitude of extreme weather events could affect a company’s supplies, operations, facilities, employees, customers and costs. After major floods in the United Kingdom in 2010, the energy utility National Grid conducted a flood risk assessment of more than 130 electricity substations and determined about 10 percent should be rebuilt or elevated. This year, as the country endured record flooding, National Grid reported that those and other investments helped minimise the impacts to its operations and customers.

Once risks are assessed, step three is to outline strategies to manage them, and pursue potential opportunities. Companies need to prioritise and integrate these measures, some of which may never have been considered before. One example of this is American Water, which provides drinking water, wastewater and related services to approximately 14 million people in more than 30 US states and in Canada. After Hurricane Floyd in 1999, the company installed a floodwall at a major plant in New Jersey that protected its facilities when Hurricane Irene came through 12 years later. But Hurricane Sandy in 2012 showed that the company needed to think beyond flood risk and build more redundancies into its telecommunications systems.

Finally, step four is to reassess risks over time, evaluating choices or changing direction as new information becomes available. For example, Weyerhaeuser, which manages more than 20 million acres of timberland around the world, uses geographic- and species-specific forecasting models and sensing technologies to monitor long-term forest growth and yield. This information helps the company adjust its strategies based on how forests respond to specific disturbances or to evolving climate conditions. One step it is taking is developing tree seedlings that could withstand summers with less water.

**Barriers to action**

A key reason more companies aren’t following suit in assessing climate risks is the lack of localised data and models that link projected climate changes to impacts germane to company operations. Companies need user-friendly, localised projections of climate change, and models that can link these projections to specific business impacts.

An important step in the right direction in the United States was the March announcement by the Obama Administration of an initiative to pull together climate data from a variety of government agencies in one place, at climate.data.gov. The initiative will not only provide better access to climate data, but also encourage the development of new tools to analyse it. The new US National Climate Assessment, which examines impacts by region and sector, will also help companies gain a better understanding of their risks.

Government also plays an important role by investing in strengthening the resilience of public
infrastructure, such as roads, bridges and ports. Of course, the real planning and implementation must be done locally. One example of leadership was the plan unveiled last year by then-Mayor Michael Bloomberg to safeguard New York City against a future Hurricane Sandy and other climate risks. Its $20bn price tag and 250 recommendations are clear indications that building resilience won’t be cheap or easy.

In many ways, building resilience is doing what companies have always done – strategic planning, risk assessment, investing in infrastructure, diversifying the supply chain and safeguarding employees – using the best information available. Leading companies are preparing to capture the competitive advantages that come from expanding these risk management practices to include the real and serious risks that accompany climate change. For many businesses, climate impacts are already imposing real costs. Waiting to act could cost even more. **RC**

**Janet Peace**  
**Vice President, Markets & Business Strategy**  
**Center for Climate and Energy Solutions**  
**T:** +1 (703) 516 4146  
**E:** press@c2es.org
HOT TOPIC

PLANNING FOR SHAREHOLDER ACTIVISM
**HOT TOPIC**

**PLANNING FOR SHAREHOLDER ACTIVISM**

**PANEL EXPERTS**

**Arthur Crozier**  
Chairman  
Innisfree M&A Incorporated  
T: +1 (212) 750 5837  
E: acrozier@innisfreema.com

Arthur B. Crozier is Chairman of Innisfree M&A Incorporated of New York and of Lake Isle M&A Incorporated, Innisfree’s wholly-owned UK subsidiary. Mr Crozier’s practice includes the representation of US and international clients in a wide variety of transactions and proxy contests, as well as annual and special meetings. In addition, he counsels an international roster of clients on corporate governance and executive compensation issues. Mr Crozier has written numerous articles and spoken extensively on the subjects of corporate governance, executive compensation, proxy contests, hedge fund activism and international voting practices.

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

Brian Hoffmann is a partner in the law firm of McDermott Will & Emery LLP and is based in the firm’s New York office. He focuses his practice on a broad range of complex corporate matters, including hostile takeovers, proxy fights, sales and divestitures, cross-border transactions, management and leveraged buyouts, acquisitions of distressed companies and domestic and international capital markets fundraising activities. He has represented acquirers, targets, financial advisors, boards of directors, special committees and other parties across numerous industry sectors, including consumer goods, energy, healthcare, life sciences, technology, media and telecommunications.

**Charles Nathan**  
Senior Advisor  
RLM Finsbury  
T: +1 (646) 805 2000  
E: charles.nathan@rlmfinsbury.com

Chuck Nathan advises global clients on M&A, financial transactions, governance, board issues and shareholder matters. Prior to joining RLM Finsbury, Mr Nathan was a partner at Latham & Watkins, where he was co-head of the global M&A practice as well as co-head of the firm's Corporate Governance Task Force. Mr Nathan represented companies and financial advisors in many significant, high-profile mergers and acquisitions, including Roche’s acquisition of the public’s minority stake in Genentech, InBev’s acquisition of Anheuser-Busch, and LiveNation’s merger with Ticketmaster Entertainment. He is the renowned author of many articles on M&A and corporate governance topics.

**Richard J. Grossman**  
Partner  
Skadden, Arps, Slate, Meagher & Flom LLP  
T: +1 (212) 735 2116  
E: richard.grossman@skadden.com

Richard J. Grossman focuses his practice on proxy contests, responses to shareholder activists, corporate governance matters, mergers and acquisitions, and leveraged buyouts. Mr Grossman has advised many companies with respect to corporate governance issues and responses to shareholder proposals. He also has represented companies in contested proxy solicitations and other contests for corporate control as well as unsolicited acquisition proposals. In addition, Mr Grossman has advised clients in designing and implementing shareholder rights plans and other corporate protective measures.
RC: How would you describe shareholder activism over last 12-18 months? What key trends have emerged? Could you comment on any recent cases of note?

Crozier: Shareholder activism has become more sophisticated in strategy, tactics and targets, as well as becoming an almost commonplace event. An activist was recently quoted as saying that five years ago he was a pariah, now he’s an asset class. One of the major catalysts has been the significant amount of capital activists have raised recently, due in large part to the significant outperformance by activist funds compared to hedge funds as a whole. Activist funds currently have approximately $100bn in AUM, up from approximately $36bn in 2009, permitting them to take on more campaigns – approximately 82 in 2013, compared to 26 in 2009 – and at larger targets, such as Apple, Microsoft and Proctor & Gamble, to name just a few. It remains the case, however, that most activist campaigns are directed at companies with market caps under $2bn. It has now become common for activists funds to hire investment banks to prepare sophisticated presentations, recruit and pay high quality director nominees, resort to litigation and wage extensive, expensive public campaigns in support of their agenda. They have also become adept at building significant positions without the company’s knowledge by using various synthetic positions. As M&A has started to come back, we have seen activists use many of the strategies and tactics honed in conventional activism in that arena as well, either to secure additional consideration, or in some cases to block the deal entirely. The leading example is the campaign last year by Carl Icahn and Southeastern Asset Management to block the going private transaction at Dell led by Michael Dell and Silver Lake Partners in favour of various alternative proposals. Ultimately, shareholders approved the going private transaction after two price increases. M&A activism also took an interesting turn recently when Pershing Square emerged as a co-bidder with Valeant Pharmaceuticals in their unsolicited proposal to acquire Allergan.

Hoffmann: Shareholder activism has continued to increase significantly. This increase is in part linked to market participants’ enhanced perceptions of activism’s legitimacy. There is greater support of activists from institutional investors and pension funds. In addition, boards of directors have become more receptive to considering activists’ proposals. Activists also have made use of social media to advance their agendas. And success breeds more activity. One of the most important trends is that the vast majority of activists’ campaigns for board seats result in the activists gaining board seats. Recent cases of note include Carl Icahn’s lobbying Apple for stock buybacks to return a
portion of its $160bn cash to the shareholders; Dell’s management buyout by its founder where Icahn and an asset management firm agitated for a better deal; Microsoft entering into a cooperation agreement with activist ValueAct, that includes appointment of activist investor’s president to Microsoft’s board; activist William Ackman’s failed efforts to revamp J.C. Penny; and Third Point’s successful campaign to add three directors to Sotheby’s board.

Nathan: Shareholder activism has become the rage of the US and, to a somewhat lesser extent, Western European equity markets over the past 18 months. Activism is daily front page news for the financial press, a number of the leading activist investors have become financial ‘rock’ stars and their names and pictures – for example, Carl Icahn, Bill Ackman, Dan Loeb and David Einhorn – are immediately recognised by a large swath of the public. The activist investor asset class has outperformed the general equity markets since 2009 and has made the returns of many conventional long/short and macro hedge funds seem puny by comparison. As a result, the asset class today is populated by about 100 separate funds which are rapidly approaching $175bn in assets under management, and no end to its growth is in sight. Moreover, the leading activists continue to show creativity, not only in target selection but also in tactics and strategy – the most recent example being the partnership of Bill Ackman’s Pershing Square fund with Valeant in a proposed unsolicited takeover of Allergan. Finally, the activists’ batting average has been increasing and may be as high as 75 percent, with activists winning many front page battles like Dan Loeb’s trouncing of Sotheby’s.

Grossman: The last 12-18 months have confirmed trends in shareholder activism that we have seen in recent years. We continue to see increasing amounts of capital allocated to activist funds and growing support for activists among institutional shareholders. As a result, activists are targeting larger, higher profile companies, driving increased media attention to activist campaigns. Recent examples include Apple, Microsoft, PepsiCo and eBay. Additionally, we see activists increasingly

“Shareholder activism has become the rage of the US and, to a somewhat lesser extent, Western European equity markets over the past 18 months.”

Charles Nathan, RLM Finsbury
utilising sophisticated tactics. Activists are stepping up their use of financial arguments and issuing white papers advocating for operational changes in the companies they target. More and more, they are also hiring experienced advisers and recruiting more qualified and credible director candidates who are knowledgeable in the target’s industry. We are also seeing a number of newer, what I call ‘son of activist’ funds being formed. These are new funds run by individuals who previously worked for and learned their trade from well-known activists such as Carl Icahn or Bill Ackman. The individuals running these funds are experienced, and they are looking to make their mark in the activism space.

**RC: What underlying market dynamics have led to the rapid growth and appeal of activist investing? To what extent are these dynamics applicable around the world?**

**Hoffmann:** New SEC rules such as those issued under the Sarbanes-Oxley Act of 2002, and say-on-pay and private ordering for proxy access which gave shareholders more power have facilitated the rapid growth of activists. Also, even as the economy has improved in the US, companies have tended to hold large stores of cash because executives are behaving cautiously. This caution results in companies remaining liquid and being reluctant to reinvest the excess cash in the business. This has negatively impacted corporate returns on equity and allowed activists to push for distribution of cash to the shareholders through stock buybacks and enhanced dividends. I believe that this dynamic is also largely applicable in other jurisdictions.

**Grossman:** Activists have been successful at targeting vulnerabilities in companies and identifying potential upside in stock prices, generating outsized returns. Consequently, a growing amount of capital has been allocated to activist funds, which enables the activists to pursue large, well-known companies. As a result, activist situations have enjoyed increased media attention, which can greatly enhance activists’ pressure on companies. Clearly, some of these developments are self-reinforcing, and they have contributed to the emergence of shareholder activism as its own asset class. To the extent that there are disproportionate ‘alpha’ returns to be made by finding and exploiting vulnerabilities in companies around the world, then the same dynamics are likely to fuel the growth of activism as they have in the United States.

**Nathan:** The rapid rise of shareholder activism is attributable to three principal factors. First is the success of the asset class since the end of the financial crisis of 2008. The average return of the activist investing asset class has consistently been in the high teens, with the top performers doing far better. Second, conventional long equity investors
need to produce performance to retain, let alone grow, assets under management. This has led to an unquenchable thirst by conventional money managers for so-called alpha returns, and this is just what activist investors produce. As a result, equity portfolio managers have become friends and allies of activist investors, not only supplying voting support in proxy contests but also funnelling activist investment ideas and opportunities to the activists. Third, activists have become more than socially acceptable. They are no longer tagged with epithets like ‘raider’ and ‘bust up’ artist. They are now widely seen as saviours who uncover inadequate or, worse, incompetent management, under-utilised capital and inefficient corporate structures and drive for solutions that create shareholder value. These factors have been at work in the US equity markets for a number of years and are spreading to the Western European equity markets, where activism is not only becoming more frequent but like the US also more socially acceptable.

**Crozier:** Among the factors leading to the growth and appeal of activist investing are unprecedented levels of cash on corporate balance sheets, the number of companies trading below their sum of the parts value and, at least in the United States, fewer structural defences and increased support by long-only institutional investors. The activists’ superior returns compared to hedge funds in general have provided them with additional capital to wage more and larger campaigns and attracted
new entrants adopting activism strategies. The underlying economic factors driving activism in the US are applicable around the world. A number of commentators are predicting a significant increase in activism in Europe, in particular. In certain markets, however, cultural and regulatory factors can inhibit, if not prevent, activism. For example, Japan has been a notoriously difficult market in which to pursue an activist strategy.

**RC: In what ways are today’s shareholders more likely to exercise their rights and challenge corporate boards? What types of issues are activist investors currently pushing?**

**Nathan:** In the US, institutional shareholders are no longer biased in favour of management, and the days of voting all proxies in accordance with management’s recommendation are long gone. Instead, institutional shareholders have well-developed internal proxy voting groups that are dominated by corporate governance specialists. Additionally, the two dominant US proxy advisory firms, ISS and Glass Lewis, are likewise focused on corporate governance best practices and have an anti-corporate establishment bias. These corporate governance specialists routinely challenge corporate boards on all types of governance issues. Activist investor campaigns can draw on this support, particularly in situations where activists identify governance problems at targeted companies and combine a better corporate governance platform with portfolio managers’ search of alpha returns to create a coalition of voting interests all too ready and able successfully to take on boards. The potency of this coalition is demonstrated by the fact that the vast majority of activist proxy campaigns end in settlement or outright victory for the activist.

**Grossman:** Traditional long-term shareholders are much more active today than they once were. Institutional investors are increasingly making their own voting decisions rather than simply relying on the recommendations of proxy advisory firms. They are also more receptive to activists and their agendas than ever before and have demonstrated both private support for activists at the ballot box, as well as public support through comments in the financial press. Some institutions have even initiated activism by encouraging activists to launch campaigns at underperforming companies in their portfolios. Meanwhile, activists are pressuring companies on a wide range of issues. While activists’ agendas were historically short-term and event-driven – for example, sales, dividends, share repurchases – we are also seeing activists focus on other areas, including strategic improvements, capital allocation, board composition, executive compensation and governance provisions viewed as ‘unfriendly’ to shareholders.
Crozier: For hedge fund activist investors, who have been dubbed ‘value investors on steroids’, the focus is on whether the stock is undervalued, whether that is due to operational issues at the company, capital allocation issues, non-core assets that can be sold or spun off or a view that it is a potential M&A target. While the tactics pursued by the activist will vary during the course of the engagement, the ultimate threat is a proxy fight to remove incumbent directors. Many conventional institutional investors, aided by third parties such as the proxy advisory firms and, in the US, the Harvard Shareholder Rights Project, have long been engaged in corporate governance activism focused on issues such as the elimination of corporate defences like classified boards, supermajority provisions, the inability of shareholders to act by written consent or to call special meetings of shareholders and the election of directors by a plurality vote standard rather than a majority voting standard. These activities, which are not necessarily related to a target company’s performance, have in many instances subsequently allowed a hedge fund activist to pursue an especially aggressive campaign at a targeted company. Notwithstanding the generally high levels of support for the newly required say-on-pay proposals, executive compensation has become an even more potent flash point for traditional institutional investors, even at well performing companies. Now that a specific vote is required on a company’s compensation program, providing a specific focus for concerns, many institutional investors are requiring direct engagement with board members on the subject, particularly with members of the compensation committee. This emphasis on director engagement is expanding beyond compensation and is increasingly touted as a way of avoiding or minimising economic activism by ensuring that the board is hearing directly from shareholders about their concerns and permitting the board to communicate their views, in turn, to the shareholders. In addition, a low vote on a say-on-pay proposal can be the fulcrum for an activist campaign, as happened at Occidental Petroleum. Relational Investors and CalSTERS announced a campaign immediately following a failed say-on-pay vote and were able to extract significant reforms as well as a board seat.

Hoffmann: I would categorise activists into two groups. One includes ‘gadflies’ or social activists who focus on social issues. The other includes financial activists who focus on the company’s economic issues and try to change the company to improve the corporate value, or stock price. With regard to the social activists, they have been pushing issues such as say-on-pay and other social issues including fair labour practices, environmental sustainability and conflict minerals – incidentally, an SEC rule related to conflict minerals was recently struck down, in part, on First Amendment grounds by a federal court. Recently, social activists have
been demanding disclosure regarding corporate political spending. The financial activists are pushing issues such as returning the company’s cash to shareholders, board and management change, including splitting the roles of chairman and CEO, and corporate restructuring including spinoffs of assets or business, by using several ways for campaigns such as proxy contest.

**RC: Activists can recruit independent director candidates by offering them incentive pay packages based on the target company’s stock performance after their election to the target’s board. What are the advantages and disadvantages of this strategy?**

**Grossman:** Director compensation arrangements with activists raise a number of issues for companies. While arrangements of the kind mentioned may incentivise performance consistent with the activist’s goals, which can be consistent with the goals of shareholders generally, many view incentive compensation as the responsibility of the company rather than outside investors. There is a danger that directors receiving outside compensation from a third-party may see themselves as owing duties to the third-party, rather than just to the company and its shareholders. If that third-party is an activist that is overly focused on short-term performance, directors may feel pressured to deliver short-term results at the expense of the company’s long-term performance. I should note that the area is still evolving. Some companies have recently adopted by-laws that limit

—

“Some companies have recently adopted by-laws that limit the ability of nominating shareholders to pay special compensation to director candidates.”

*Richard J. Grossman, Skadden, Arps, Slate, Meagher & Flom LLP*

...
clear how common these arrangements will become going forward.

**Hoffmann:** The advantage is that the incentive pay packages will help the activists to recruit qualified individuals as a director candidate and to align these directors’ economic interest with the activists. The disadvantage of the incentive pay packages is at a minimum the appearance of a conflict of interest, because these packages are typically paid by the activists and not the corporation. This makes these directors beholden not to the corporation and its shareholders but to the activist. It also can set up a negative dynamic of having effectively two classes of directors. In at least one instance, an incentive pay package for an activist’s nominee was dropped in the face of a negative market reaction.

**Crozier:** The activist can position such payments, which are often referred to as ‘golden leashes’, as a demonstration that his or her nominees’ interests are directly linked to those of other shareholders and thereby better suited as directors than management’s nominees. Management, however, has potentially powerful counter arguments, such as that these arrangements can incentivise excessive risk taking, particularly if there is a time limit on the package, and that they can inhibit collegiality among board members. In the Agrium/JANA Partners proxy fight last year, Agrium, which is a Canadian company, successfully persuaded many non-US shareholders that the JANA pay package was contrary to Canadian standards applicable to directors’ fiduciary duties which require directors to consider the best interests of the enterprise as a whole and not just those of shareholders, the applicable standard in the US. It should be noted, however, that many US companies which adopted by-laws precluding a nominee director from being compensated by a third party have subsequently dropped such provisions due to opposition by ISS which stated that it might recommend a vote against directors if the provision was adopted without shareholder approval. ISS, however, does not object to a by-law precluding a director nominee for failure to disclose a third-party compensation arrangement. In ISS’s view, such by-laws promote transparency and better-informed voting decisions.

**Nathan:** The obvious advantage of the strategy is that offering financially meaningful incentive pay to director candidates should help activists convince highly talented business persons to accept the reputational risk of participating in what could be a bruising proxy contest and to commit the time and effort to being a strong proactive director on the target’s board. For candidates of this type, a director’s annual compensation, even at a very large public company, may not be convincing. Giving a nominee an opportunity to achieve truly large incentive returns for aggressively pursuing programs
aimed at increasing shareholder value creates a win-win scenario for an activist investor. On the other hand, paying activist-nominated directors differently from other directors creates at least an appearance of possible conflict. Critics of incentive pay for activist directors, including a number of institutional investors and corporate governance specialists, point to the divisiveness it could easily create in the boardroom, as well as the fact that the incentive pay packages seen to date have been linked to a rise in stock price over a relatively short – say, one or two year – period.
**RC:** Some types of activism seem to chase a short-term stock price boost while others aim to achieve long-term, sustainable growth. How should different activist agendas affect a board’s strategic response?

**Crozier:** In many ways, the board’s strategic response is the same, whether the activist is pursuing a short- or long-term agenda. In either case, the company must be able to effectively argue that its current strategy will create greater shareholder value than the activist’s within a reasonable timeframe. If that is not feasible, then the company needs to carefully consider its vulnerability in a possible proxy fight and, if vulnerable, whether to adopt some of the activist agenda in order to preclude the fight or increase the odds of success. If the latter, it is beneficial if the company has already done a self-assessment and determined to take that action so as not to appear purely reactive.

**Hoffmann:** There has been an ongoing debate regarding the long-term effects of activism. Some claim that activists who seek a short-term stock price boost demand actions with short-term benefits at the expense of long-term interests of the company and its shareholders. According to this theory, the initial stock price boost is caused by the failure of the short-term market prices to correctly reflect the long-term cost associated with such action taken by the company. Meanwhile, some academics claim that there is no data that evidences the above claim. From my perspective, this theory seems counter-intuitive in that it is based on the market being incapable of pricing in the long-term damage that management clearly sees. Enlightened boards should ignore the fact that a proposal came from an activist. The board should consider whether what the activist proposes is in the company’s and shareholders’ best interest.

**Nathan:** There are no cookie-cutter responses to an activist campaign, whether it is geared to a short-term price boost or to long-term, sustainable growth.

“Because of the growth of shareholder activism in recent years, if a company fails to respond to activists properly, the reputation of the company with investors could be damaged.”

*Brian Hoffmann, McDermott Will & Emery LLP*
growth. Indeed, the short-term versus long-term debate is often a red herring. The key to a successful activist defence is a board-backed program which in the eyes of its investors will create greater present shareholder value. For example, a board might argue that its long-term strategy should not change because, even taking account of execution risk, it will create more value for shareholders, on a present value basis, than the activist’s short-term program. If this argument is convincing, the shareholders will back it. On the other hand, a board might argue for a relatively short-term value creation program, on the grounds that its value creation is higher than a longer-term strategy proposed by the activist after taking into account execution risk and time value of money. At the end of the day, the investors will act as a jury and a majority will vote for the business plan it believes offers a higher present value opportunity without regard to short-term and long-term labels.

**Grossman:** It is important to recognise that not all activists are the same. While companies must remain on their guard, they should also plan with an open mind and should not assume that all activists are hostile. Some activists are driven by short-term agendas, but others may be constructive and willing to work with companies for long-term improvements. It is critical to research prior campaigns to understand a particular activist’s modus operandi and to anticipate next steps. Companies should take the ‘high road’ in responding to activists and be prepared to meet and consider proposals. Meetings with activists can be productive and can provide an opportunity to explain the company’s strategic plan while hearing a fresh perspective. Depending on the company’s response, an activist may even discover that its original thinking was wrong.

**RC:** When facing shareholder activism, how important is it for a board to develop an effective communications plan? What financial and reputational impact can this process have on the company?

**Hoffmann:** It is essential for a company to regularly communicate with its shareholders even in the absence of an activist campaign. It is equally as important for a board to develop an effective communications plan when facing shareholder activism. Because of the growth of shareholder activism in recent years, if a company fails to respond to activists properly, the reputation of the company with investors could be damaged. When a company receives a proposal from activists, it should first impartially consider the merits of the proposal. If the company considers that the proposal is not in the company’s and its shareholders’ best interest based on its analysis, then it should clearly articulate why the proposal is not in the company’s and its shareholders’ best interest and communicate its analysis to the shareholders.
**Nathan:** An effective communications plan is essential to a successful activism defence. An activist campaign is quite simply a contest for the hearts and minds of a majority of the investors. Like a modern political campaign, a target cannot win activist campaign without an effective communications plan effectively implemented. A target board may have a far better business plan than an activist, but unless it is communicated to the shareholders effectively, it will not prevail. A failed communications plan means a loss of the activist contest.

**Grossman:** It is crucial that companies develop and maintain an effective communications plan in preparation and response to activism. Today’s fights are increasingly won or lost through public relations, rather than the use of legal defences. Consequently, companies should invest the time and effort to stay fully engaged with shareholders and clearly communicate strategies for long-term shareholder value. Companies should also listen to shareholder concerns. While this is primarily a role for management, it may at times be appropriate for individual directors, in coordination with management, to meet with large shareholders and seek to understand their perspectives. Ongoing communication and shareholder engagement provide institutional investors with greater familiarity with the board and management. This helps to establish credibility and build confidence in the board’s strategy. A company facing shareholder activism should be mindful that the activist has likely already reached out to other shareholders well in advance of initiating a public campaign. Accordingly, the board and management should be proactive in presenting their vision and long-term strategy for the company as a superior alternative to the activist’s agenda. These efforts may well determine the result of a contested solicitation.

**Crozier:** In activist engagements, management’s credibility with shareholders is essential to success. Accordingly, the company must have a communications program that credibly, clearly and concisely demonstrates that the board and management are committed to shareholder value and that their strategy will produce greater and more certain value than the activist’s. If the overall communications program and details underlying it are not credible, significant financial and reputational harm can result.

**RC:** Could you outline some of the common response strategies that might be used by a company that has become the target of an activist campaign? What general advice can you offer to board members in these circumstances?

**Nathan:** By and large, today’s investors sympathise with activists. Trying to persuade
In activist engagements, management’s credibility with shareholders is essential to success.”

Arthur Crozier,
Innisfree M&A Incorporated

investors that the activist is just a ‘bad guy’ will be counter-productive. This is not to say that an activist’s track record is off-limits, but that it is important only in so far as it is persuasive on the merits of the activist’s proposed program. Boards should not brush off activist approaches or requests for a meeting, nor should management be permitted to do so. Boards should not assume that every activist has evil motives or wants a public fight. As in most walks in life, activists come in all shapes and sizes. Research your opponent and keep an open mind. Remember that peace, even at a price, may be far better than war. It is also important for a board not to blindly accept management’s evaluation. Even the best strategic plan or operational proficiency may be open to improvement. Remember that management does not have a monopoly on wisdom, and an activist may have good ideas that have not occurred to management or have been inappropriately dismissed. A dialogue with an activist with board participation before war is declared – preferably before the activist has gone public – is ideal, whether or not it leads to a solution. At worst, the board will be able to take the measure of the activist and its ideas, and at best the parties may find a peaceful and constructive resolution that creates a proverbial ‘win-win’.

**Grossman:** The company should first assemble an advisory team as soon as possible, consisting of legal counsel, financial advisers, public relations specialists and proxy solicitors. In consultation with its advisers, the company should next increase its engagement and communication efforts. The activist is likely to have already reached out to institutional shareholders, so it is helpful if the company has already built strong investor relationships and is not engaging shareholders in a meaningful way for the first time after an activist surfaces. The activist may request a meeting with management. We generally advise companies to take the meeting with the activist. Engaging with an open mind provides a chance to learn who the company is dealing with and may present an opportunity to work together for improvements that benefit everyone. Much depends on the particular activist’s end goals. Many
companies faced with an activist who is threatening an election contest have been more willing to consider entering into settlement agreements under the right circumstances. Particularly in situations where traditional ‘long’ institutions with large stakes are supporting change, proxy settlements can be an option that spares companies the publicity, expense, distraction and increased uncertainty of a long, drawn-out fight. In an election contest, a settlement allows the company to have some say in the selection of the new directors, as well as which directors, if any, go off the board.

**Crozier:** The response strategy depends on the company’s assessment of its vulnerability. If the company believes that the activist’s program is unlikely to gain traction with shareholders, the response strategy is likely to be direct engagement
with investors, the sell side, the media and other relevant constituencies advocating the company’s superior strategy to deliver shareholder value and pointing out the flaws in the activist’s strategy. If, however, the activist’s program is likely to be well received, the board needs to consider various alternatives, such as adopting part or all of the activist’s program, adding new directors to the board, possibly including directors proposed by the dissident, or the formation of a special committee tasked to review strategic alternatives. They should also meet with the activist, if only in listen-only mode, so as not to appear entrenched. In determining which response strategy to pursue, the board needs to keep in mind that the most important constituency in an activist campaign is the shareholders. While there are numerous other constituencies, such as employees, vendors, customers, regulators, the only goal is to win the hearts and minds of the key shareholders. The strategy towards the other constituencies must be consonant with, and supportive of, the shareholder focused strategy.

Hoffmann: Communication is the key for a company that is the target of an activist investor, so my general advice to the board members would be to establish an explicit strategy for communication with the shareholders. Moreover, as soon as an activist investor takes any action regarding the company, the board and its management should organise a team with a small number of members, including experienced outside experts. Once the company decides how it will deal with the activist’s proposals, the small team should ensure the coherence of the communication strategies and respond to the activist actions in a timely manner as well as keep the full board fully informed. The team should also make sure it is responsive to questions and concerns of investors.

RC: What action should companies take to prepare for the possibility that they may become the target of an activist investor? How can firms take positive steps to pre-empt activism?

Grossman: Companies must remain vigilant and prepared for shareholder activism. As discussed, engagement with shareholders is more important today than any legal defence. In addition to building shareholder confidence in the board and management and their strategy to create value, engagement provides an opportunity to address investor concerns before they become problems. Companies should also monitor who is accumulating their shares. They should review who is on calls with investors, examine 13F filings and keep stock watch programs. Additionally, companies should conduct regular vulnerability assessments with their financial advisers to identify and ameliorate factors that might attract an activist. These include,
among other things, a lower price-to-earnings ratio than peers, excess cash on the balance sheet, operational underperformance relative to peers, an underleveraged capital structure and divestible non-core assets. Companies should also be aware of governance vulnerabilities, such as a lack of board independence or core competencies, provisions that favour management and the board vis-à-vis shareholders, and compensation for executives or directors that is significantly higher than peers. More and more companies are understanding the importance of shareholder engagement and efforts are being made to strengthen their shareholder relations. Companies and boards are increasingly paying more attention to, and having constructive dialogues with, their largest shareholders in order to better understand investor perspectives on performance, strategy and governance, and to consider changes as appropriate.

**Hoffmann:** Companies should communicate with their shareholders regularly and make sure to listen to their concerns. In addition, a company should consider taking pre-emptive actions based on its self-assessment. For example, a company with excess cash should consider undertaking its own analysis regarding a possible distribution to the shareholders or buyback before becoming the target of an activist investor. If the company distributes cash to the shareholders in the manner and amount determined based on the company’s own analysis, then it will be less likely that activists will attack the company proposing distribution of excess cash to shareholders and even if they do attack, the company can make a strong argument against the activist’s proposal.

**Crozier:** The best advice for board members is to be prepared in advance of an activist campaign. They should oversee a candid assessment of the company’s vulnerabilities – do shareholders or the sell side believe the company is undervalued; is the company’s stock price underperforming that of its peers; is there excess cash on the balance sheet; are there non-core assets that are a drag on earnings; is the sector subject to increased M&A activity; and so on. They should also retain a stock monitoring firm with the expertise necessary to identify likely accumulations by activists, including through synthetic positions. In addition, they should define the core messages and establish and communicate to shareholders measurable goals related to those metrics that will drive shareholder value. The company needs to maintain regular communications with key shareholders – ensure that they understand the company’s strategy and do not let misunderstandings or concerns fester unaddressed. In-person engagement with senior management is far superior to telephone calls or emails. It is also important to establish a clear communications strategy that limits who can speak to external parties to ensure consistency of messaging. The
board should also consider the composition of the board, whether the existing members have the skill set required to effectively oversee the company’s strategy. In that regard, director tenure, in particular, has become a particular focus for activists, as well as traditional institutional investors. It is much better to deal with a board transition in a voluntary, controlled fashion, rather than through a proxy fight.

Nathan: The key to advance preparation is to ‘know thyself’, not through the magic mirror of the wicked witch in Snow White but in the cold light of the real world. Armed with this self-knowledge and a truly open mind, review the company’s strategy and performance and, putting yourself in the shoes of an activist, ask what could be done to create additional shareholder value. Unfortunately, this type of preparation is easier said than done. To facilitate such an objective self-examination, a board should retain an experienced independent financial adviser and charge it with conducting a third party review of the company’s business and strategy – in effect, put itself in the shoes of an activist and evaluate the company from an activist’s perspective. Another important facet of preparation is learning what your investors really think, not what you hope they think and not even what they may say to you. Another cardinal rule for effective advance preparation is to assemble a skilled and experienced advisory team and request the team to prepare not just management, but also the board, for the potential of an activist investor campaign. This is often achieved through adviser-created role playing exercises for management and the board intended to illustrate the realities of an activist attack. However, all of the foregoing preparation will be of little avail if the company does not address its identified weaknesses proactively. RC
1stWEST Financial Corporation provides background investigations, asset searches and fraud investigations for the corporate finance industry and other professionals in need of satisfying their background due-diligence requirements on prospect companies, principals, senior managers, partners and overviewkey management personnel. Founded in 1991, 1stWEST provides information to assist our clients in investment due-diligence and underwriting, contract negotiations, litigation resolution and pre-employment requirements by providing information to determine the financial character and capacity of the business or person with which they are dealing or employing. In the financial services sector, our extensive experience in background investigations, banking, corporate and real estate finance enables us to provide superior products and service in this area of specialization.
In today’s global market, a multijurisdictional approach to compliance is essential. With offices in key financial centres and emerging markets, Baker & McKenzie lawyers are already on the ground, ready to tackle investigations. Our approach ensures that your compliance program satisfies the expectations of enforcement authorities around the globe, providing protection where you need it most.
Berkeley Research Group, LLC is a leading global expert services and consulting firm that provides independent expert testimony, litigation and regulatory support, authoritative studies, strategic advice, and document and data analytics to major law firms, Fortune 500 corporations, government agencies, and regulatory bodies around the world. From testifying in high-stakes litigation to consulting on large-scale projects, BRG experts and consultants combine intellectual rigor with practical, real-world experience and an in-depth understanding of industries and markets.

Richard Fogarty
Director, Latin America Practice Leader
New York, NY, US
T: +1 401 824 4097
E: rfogarty@brg-expert.com
Bretton Woods Law is a set of barristers Chambers whose members focus solely on International Organisations Law. Our members specialise in representing companies facing possible sanctions, including debarment or more serious repercussions by Multilateral Development Banks, as a result of an investigation into or an allegation of engaging in, sanctionable practices. Bretton Woods Law has world-class credentials in this field and can provide a wide range of appropriate solutions to best defend companies’ interests. Our members have particular expertise in negotiating resolution or settlement agreements and are adept at assisting companies to fulfill their obligations thereafter.
Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority – no matter what the industry sector is. With more than 2600 fraud investigation and dispute professionals around the world, EY assembles the right multidisciplinary and culturally aligned team to work with you and your legal advisers. We work to give you the benefit of our broad sector experience, our deep subject matter knowledge and the latest insights from our work worldwide.
**Goodwin Procter**

Goodwin Procter's Labor & Employment practice counsels and litigates on behalf of employers with respect to all aspects of the employment relationship, including employee mobility disputes, Fair Labor Standards Act compliance, executive compensation disputes, workplace violence, disability and leave of absence matters, employee privacy concerns, sexual harassment and other discrimination issues, duty of loyalty disputes, employment agreement negotiation and disputes and collective bargaining matters, among others. We combine in-depth legal knowledge with focused, practical experience to help managers make real-world judgments while minimizing potential exposure.
Innisfree M&A Incorporated (New York)
and its wholly-owned subsidiary Lake Isle M&A
Incorporated (London) provide clients with
sound tactical and strategic advice and results-
oriented implementation in proxy solicitations,
tender and exchange offers, mergers, rights
offerings, restructurings and other corporate
actions – friendly or contested, domestic or
cross-border. In addition, we provide consulting
services on strategic management issues,
such as corporate governance, executive
compensation and investor relations. With an
experienced professional staff in New York,
London, and Pittsburgh, we have represented
hundreds of companies in over 20 countries.
Poyner Spruill’s Privacy and Information Security team knows that information is a vital asset of any business. Our practice focuses exclusively on privacy, information security, and records management law, and matters such as breach response, online and mobile privacy, marketing, vendor management and other areas of compliance and risk. We provide comprehensive, practical services to clients from a variety of industries including health care, clinical research, financial services, insurance, retail, utility, technology, consumer goods and client services. As a mid-size firm, we support clients of various size and scope, ranging from Fortune 100 companies with international reach to local charities.
RLM Finsbury is a global leader in strategic communications and a trusted adviser to boards of directors, senior executives and legal counsel of many of the world’s most successful companies, institutions and organisations. The firm has managed some of the most complex communications challenges, financial issues, reputational matters and other corporate crises of the last three decades. These include high-profile litigation, mergers and acquisitions, executive changes, restructurings and proxy fights, as well as brand positioning campaigns, product launches, advocacy campaigns, congressional investigations, legislative initiatives, labour matters, regulatory reviews and long-term reputation and employee engagement efforts.
Shearman & Sterling has been advising many of the world’s leading corporations and financial institutions, governments and governmental organizations for 140 years. We are committed to providing legal advice that is insightful and valuable to our clients. Together, our lawyers work across practices and jurisdictions to provide the highest quality legal services, bringing their collective experience to bear on the issues that clients face. For example, underpinning the quality of our work firmwide are our shared values. We take pride in the successes of our clients and in our contributions to them.
The Cambio Consulting Group was founded by Dr Douglas Webster to help organisations improve competitiveness and maximise stakeholder value by understanding and proactively leading change. Services include strategic planning, cost management, performance management, enterprise risk management, organisational change management and the integration of those through a proprietary framework designed to improve overall organisational value.

Dr Doug Webster
President
Dumfries, VA, US
T: +1 (703) 441 2212
E: dougwebster@cambiocg.com

www.cambiocg.com

Giving Voice to Values (GVV) is an innovative approach to promoting a higher level of integrity through business education and in the workplace, pioneered by Dr Mary C. Gentile. Launched by The Aspen Institute and the Yale School of Management, GVV is now based at Babson College. Drawing on experience as well as scholarship, GVV is not about persuading people to be more ethical. Rather GVV starts from the premise that most of us already want to act on our values, but that we also want to feel that we have a reasonable chance of doing so effectively and successfully.

Mary C. Gentile
Director, Giving Voice To Values
Boston, MA, US
T: +1 (781) 648 3220
E: mgentile3@babson.edu

www.babson.edu
**ORGANISATION**

**C2ES – the Center for Climate and Energy Solutions**

**C2ES** – the Center for Climate and Energy Solutions – is an independent, nonpartisan, nonprofit organization working to advance strong policy and action to address the twin challenges of energy and climate change. Launched in November 2011, C2ES is the successor to the Pew Center on Global Climate Change, long recognized in the United States and abroad as an influential and pragmatic voice on climate issues. At C2ES, we believe that ensuring safe, reliable, affordable energy for all – while protecting the global climate – is a paramount challenge of the 21st century.

**Janet Peace**  
Vice President, Markets & Business Strategy  
Arlington, VA, US  
T: +1 (703) 516 4146  
E: press@c2es.org

www.c2es.org

---

**ORGANISATION**

**Reputation Institute**

**Reputation Institute** is the world’s leading reputation management consultancy, enabling leaders to make more confident business decisions that build and protect reputation capital and drive competitive advantage. Our most prominent management tool analyses the reputations of companies and institutions. Businesses and executives regularly discover best practices in reputation management by affiliating with our Knowledge Center and participating in its learning programs and networking events. Reputation Institute has offices and associates in 30 countries around the world.

**John Patterson**  
Senior Advisor  
New York, NY, US  
T: +1 (212) 495 3855  
E: jpatterson@reputationinstitute.com

www.reputationinstitute.com