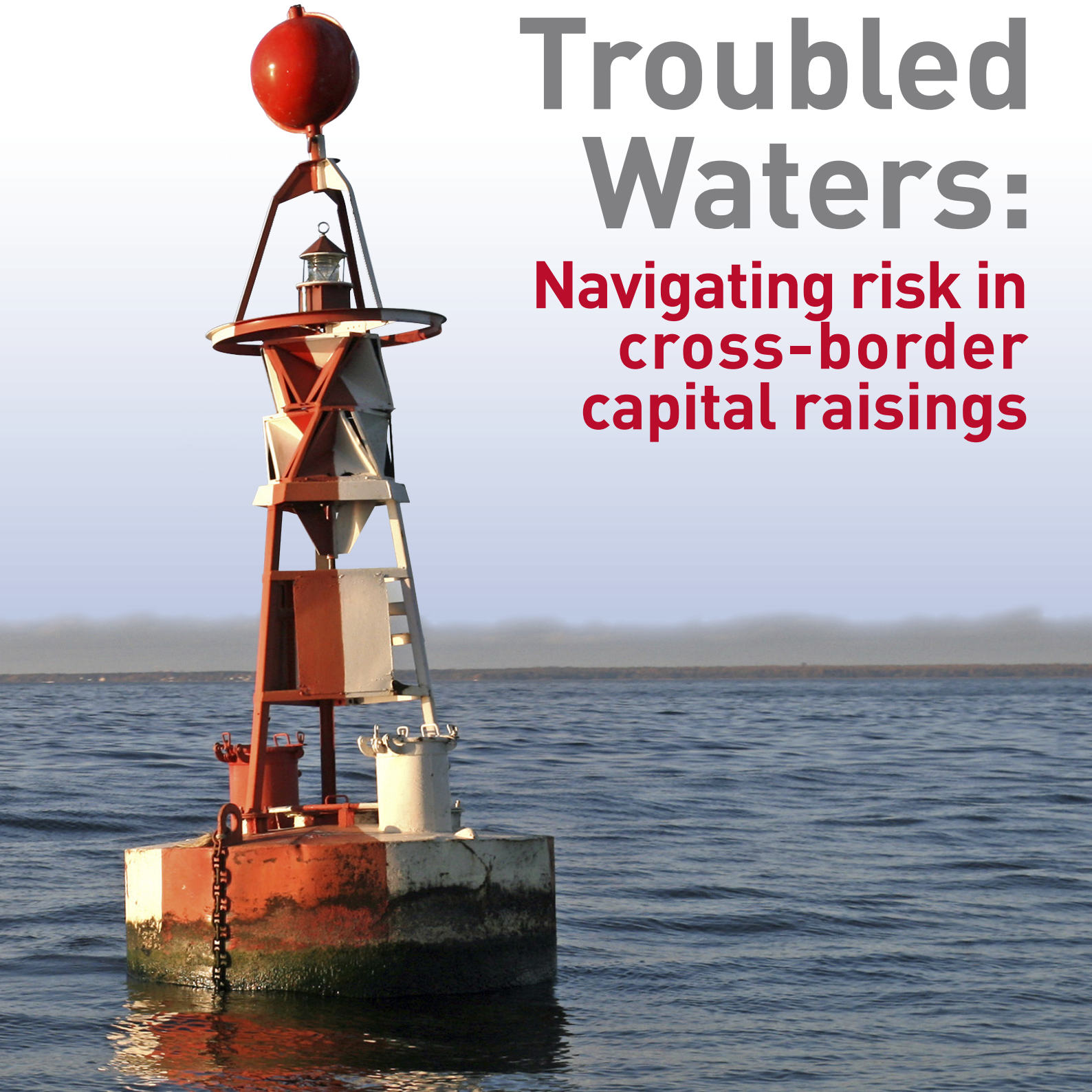
Baker McKenzie.



Troubled Waters:

Navigating risk in cross-border capital raisings

A **note** from Baker McKenzie

The global financial crisis fundamentally changed attitudes toward risk. As financial giants fell and governments flirted with bankruptcy, many investors were unwilling to risk capital on new ventures. Capital markets have regained much of this lost vitality and the number of initial public offerings (IPOs) undertaken by companies has risen significantly in 2014. Nevertheless, as the year has progressed, investors have demonstrated a degree of "deal fatigue." While the window for new IPOs remains open, investors are much more discerning about where to stake their capital.

To a great extent, this selectivity is attributable to that renewed appreciation of risk and has made the cleansing sunlight of transparency an essential component of any capital-raising. While companies have long been subject to obligations to disclose business-critical information in their offering documents, those disclosures are now receiving even greater scrutiny. Investors seek a better understanding of the issuer's business and the drivers of its profitability, while regulators are intensifying efforts to ensure that issuers comply with their legal disclosure requirements.

This desire for transparency is particularly relevant in cross-border deals or where issuers have significant operations in emerging markets. In this report, we partnered with political and security risk consultant Global Torchlight to provide an overview of some of the risk factors attracting particular attention from investors and regulators or that are otherwise relevant to companies operating in emerging markets. It offers practical guidance on how companies can better assess the risks applicable to their business and manage their disclosure in ways that demonstrate a considered understanding of their impact. It also shows how comprehensive assessment of these external risk factors can be used to develop a strategy with which to mitigate them and improve returns for investors. Adoption of such an approach to the assessment and disclosure of risk can yield significant benefits for companies raising money on international capital markets.

We hope you find this report to be useful as you consider raising capital outside of your domestic markets.

Koen Vanhaerents
Chair, Global Capital Markets Practice Group
Baker McKenzie

Contents

Executive Summary

This report serves as a guide to some of the critical external risks that companies may encounter as they do business around the world, particularly in emerging markets. Countries that, only a few years ago, had some of the highest long-term growth potential have gone on to experience substantial political and security-related challenges. These events may not have eliminated business opportunities completely, but they have invariably changed the environment in which companies pursue them.

The report begins by briefly outlining the legal foundations of disclosure and some of the basic principles for companies to consider when embarking on the process of raising capital on international financial markets ***(The Disclosure Exercise)***. Next, it offers practical advice on how issuers can manage the process efficiently and effectively, so as to maximize its value to the issuing company ***(Practical Guidance: From Identification to Mitigation)***. It then provides a comprehensive assessment of a number of external risk factors that are particularly relevant in emerging markets or that are attracting the attention of securities regulators ***(Disclosure Hot Topics)***. Specific recent examples of each of these issues are included for illustrative purposes.

As will be seen, the risks considered here do not apply universally around the world, nor do they impact businesses in a uniform fashion. Some of these risks will be immediately apparent to readers, while others will only become fully evident after further evaluation. Some will not be relevant to a particular country or industry, while others are evolving rapidly and in sometimes unpredictable ways.

Drawing on the detailed knowledge of local advisors with the experience and understanding of these issues and their broader contexts will enable companies to apply these general risk factors to their own particular businesses and circumstances. In gaining a better understanding of trends in geopolitical risk and in how investors and regulators are viewing them, companies can measure the adequacy of their own disclosures and the extent to which they are taking full advantage of the benefits offered by the disclosure process.

The Disclosure Exercise

Every kick-off meeting for a capital markets transaction includes "The Speech." Counsel will inform the issuer's management team that their prospectus is a "liability document," designed to protect the issuer from investors claiming that they were not fully informed about their investment. The Speech will emphasize the need for a conservative approach to disclosure as the prospectuses will, as a practical matter, be judged in hindsight in light of post-offering events. Management will be told that disclosure should be tailored to the business and not generic. Risk disclosure should be presented in order of importance and without mitigating factors that undermine the risks' warning.

Putting pen to paper, the lawyers usually begin by stitching together sections from precedent prospectuses from other issuers into a first draft for discussion with management. If the issuer is from an emerging market, a special section highlighting country-specific risks is included in the prospectus. These country risk sections are used over and over, updated for current events and whittled down as the country develops and investor knowledge of the market grows.

The use of precedents provides a great deal of comfort to issuers. If you disclose all of the same risks as everyone else in your industry, it seems like it should be harder for a claimant to identify a deficiency. However, over-reliance on previous prospectuses or on others' disclosure is not ideal. The operating environment can be remarkably fluid; events can occur at a dizzying pace with effects far beyond their point of origin. The wave of uprisings and political unrest that constituted 2011's "Arab Spring" made this abundantly clear, with the full effects of the turbulence still to be determined.

Investors often review a prospectus with some understanding of the external factors relevant to businesses in a particular country or region. They look to the disclosures to provide them with a company's perspective on such issues. Disclosures that are current and tailored to a company's business can help to provide investors with assurances that the company has undertaken a comprehensive risk assessment as part of the transaction.

Practical Guidance: From Identification to Mitigation

For many companies, especially newer ones, the disclosure process may have benefits beyond the capital markets transaction involved. Carefully considering the internal and external challenges to the business gives companies an opportunity to implement or refresh their corporate risk management procedures. By adopting a number of the following practical guidelines, companies can ease the disclosure drafting process while enhancing its overall value to the prospectus and to the company's risk management strategy.

Managing the Disclosure Exercise

Start the Process Early

Analyzing the current risk environment early in the transaction provides opportunity for more careful consideration of risks and their potential impact.

Monitor Changes During and After the Transaction

Disclosure obligations last through to closing. Changes can and do occur even during the investor meeting phase. Continual monitoring of risks, including external risks, is essential.

Anticipate Questions

Companies should prepare for questions relating to external developments, which may come from a range of third parties, including lenders, investors (both current and prospective), underwriters, suppliers, customers, insurers, and even non-executive board members.

While companies may not always be able to downplay a particular political or security risk, they can often further assuage concerns by pointing to a comprehensive internal risk management strategy to deal with such challenges should they arise.

Effective Risk Management

Learn to Anticipate Crises

The disclosure process will, among other things, refine the thinking of a company's board and management about the external factors most likely to impact the business in the future. This, in turn, will allow them to accurately determine whether the company can respond to potentially harmful events.

Specific responses to potential crises will depend on a range of circumstances unique to the company and its business. In order to develop them, a company must ask itself the right questions, which will be made apparent by a thorough risk assessment. Examples include:

- To what extent will regional conflict disrupt deliveries from suppliers or inhibit the ability to dispatch products to customers?
- Will the company's business be impacted by the election of a government that is hostile to foreign investors?
- Is a company perceived as closely aligned to an unpopular political leader and, thereby, a target for protest itself?

Anticipating potential risks allows a company to engage the relevant components of its organization and to develop contingency plans for such scenarios. This process will involve not only operational managers, but also legal, financial, human resources, and communications teams, among others. Such a collective planning effort will leave the company far better prepared to respond to unforeseen circumstances and manage their potential consequences.

Board Level Risk Assessment

Companies should consider establishing a board level risk committee that will review and monitor risks on an ongoing basis.

Link Disclosure to Anti-Corruption Compliance

In the wake of the global financial crisis and with global emphasis on corporate social responsibility growing, companies around the world are subject to new initiatives aimed at countering corrupt practices and enhancing corporate governance. Many of these are far-reaching, covering a company's suppliers and partners. The financial advisors to a capital markets transaction will require representations and warranties from the issuer as to compliance with these regulations.

The disclosure exercise will force companies to consider the application of these laws, and is an opportunity to start an ongoing monitoring process. Best practice would be to test compliance at least annually.

Analyze the Adequacy of Insurance Coverage

Companies should consider altering the level and type of insurance coverage carried, in order to reflect risks identified in the disclosure process. While companies will carry general coverage to protect against a broad range of risks, more specialist forms of insurance are also available including:

- Kidnap & ransom (K&R) coverage for companies operating in regions where terrorism or kidnapping is prevalent, and
- Political risk insurance (PRI) to cover losses incurred due to a range of circumstances, from the expropriation of assets to the consequences of political violence and civil unrest to the imposition of currency controls or the occurrence of a sovereign debt default.

Disclosure Hot Topics

Local Partnership and Associational Risks

In an age of mass social media and instantaneous communication, a company's reputation is a valuable asset in and of itself. A corporate reputation can take years to build but can suffer substantial damage quickly if it is not adequately and actively protected. Businesses must prepare to take immediate action to mitigate any threats to their reputations.

In preparing disclosures, companies will naturally focus on the events and risks that could have a material impact on their financial position. However, given the possible consequences of reputational damage on long-term profitability, prudent managers should also adopt an objective perspective when assessing vulnerabilities. They should consider:

- how the conditions in which their company operates might be perceived by those outside the company, and
- whether these perceptions could present material challenges to the company's reputation.

When companies enter new and unfamiliar markets, they often work with a local partner, either to share risk or to benefit from local knowledge. In other cases, local law might require them to establish their operations in conjunction with a local individual or company.

Businesses already recognize the importance of conducting due diligence on such partners in order to satisfy internal compliance policies and relevant anti-corruption and bribery laws. However, they should also consider the reputational consequences of association with a partner. This is especially relevant where companies work with government entities or officials, since such relationships can be perceived by outside observers as support for or endorsement of that particular government's policies.

For instance, it is a relatively common practice for resources companies to partner – either by choice or as a condition of their investment – with local police or military forces to provide site security for facilities. While many companies in extractive industries have signed up to voluntary protocols governing the management of such relationships, their control over the way in which contracted security obligations are carried out is often limited. In a number of countries, concerns have been raised about the potential

Case in Point: Local Partnership and Associational Risks

In 2011, workers for the state oil company in the western Kazakhstan city of Zhanaozen went on strike for better pay and working conditions. Many of the strikers were fired after a local court ruled the strike illegal, but the protests continued.

In December 2011, while attempting to clear protesters from Zhanaozen's main square, police opened fire, causing a number of fatalities. Kazakhstan's government quickly sought to quell the risk of further violence by making concessions to the strikers, replacing certain local officials, and charging some police officers for their role in the incident.

Many foreign energy companies operating in Kazakhstan became concerned that labor unrest would spread from the state sector. In such circumstances, they would have little to no control over how the authorities might respond, but would have suffered potential reputational damage if further violence had been used.

The incident at Zhanaozen also prompted renewed criticism from foreign NGOs to distance themselves from the Kazakhstani government.

for human rights violations to be committed by those forces while carrying out duties on behalf of foreign companies. In those circumstances, companies can still suffer severe reputational damage despite their lack of control.

Equally, advocacy groups and non-governmental organizations have targeted companies for their relationships with governments that are perceived as persistent violators of human rights or that are otherwise the subject of concern for their behavior. This can affect a company's reputation elsewhere, including in its own home.

With so much potentially at stake, gaining a comprehensive understanding of local events and conditions and considering them from an outside observer's perspective becomes all the more critical. This gives companies the opportunity to assess potential associational threats to their reputation that local events could trigger. Even if a company decides that such issues do not warrant disclosure, the assessment of potential second-order risks allows it to anticipate problems and put contingencies in place should they arise.

Bribery and Corruption

Many companies doing business internationally will already be familiar with the risks associated with bribery and corruption. The past decade has seen a substantial rise in the number of prosecutions of companies under laws such as the US Foreign Corrupt Practices Act (FCPA). Corporate counsel now consistently rate compliance with such laws as one of the most significant risks that a multinational company faces.

Nevertheless, official corruption remains an unfortunate fact of life in many countries. In the 2013 edition of its annual Corruption Perceptions Index, Transparency International reported that almost 70 percent of the 177 countries surveyed scored low enough to be perceived as having a serious corruption problem.

Increased enforcement of anti-bribery and corruption laws is the most overt way in which many governments have sought to put pressure on multinational companies to avoid engaging in such activities. However, many companies are looking much more holistically at how they manage that compliance risk. This includes assessing whether doing business in countries where corruption is prevalent triggers obligations to make disclosures in securities listing documents.

Excluding materiality, in the absence of legally mandated disclosure requirements, companies will want to work with their legal counsel and other advisors to determine whether individual circumstances and relevant market practice warrant disclosure of bribery and corruption-related risks. Many factors will influence that determination.

Case in Point: Bribery and Corruption

Businesses have had to contend with the risk of corruption in Libya for some time, even following the removal of Muammar Gaddafi from power. Transparency International ranked the country 172nd out of 177 surveyed for its 2013 Corruption Perceptions Index, a decline of 12 places from its ranking in 2012.

However, the presence of corruption can generate other, even more acute risks. In 2013, rebel groups seeking greater autonomy for Libya's eastern Cyrenaica region closed off access to critical oil export terminals in that part of the country. Among their demands for reopening the ports were calls for independent investigations into allegations of official corruption in the country's energy industry. The blockades lasted for over six months, during which time Libyan oil exports plummeted by almost 80 percent.

This incident had significant implications for Libya's economic growth. It also galvanized the issue of corruption in the eyes of the Libyan people and renewed international focus on the broader security and risk challenges that Libya faces in its post-Gaddafi development. It serves to demonstrate that corruption, or even its allegations, can produce further layers of political and security risks that companies must contend with and that extend well beyond the compliance obligations they are most familiar with.

These include:

- Assessing the state of the company's compliance program and its implementation of the five essential elements: (i) leadership; (ii) risk assessment; (iii) standards and controls; (iv) training and communication; and (v) oversight. Many institutional and other activist shareholders now demand compliance in these areas and the risk of class actions and shareholder litigation regarding the state of the compliance program and its implementation is a tangible threat when things go wrong.
- Regulators consider operating in a market with known corruption challenges a compliance "red flag" and a host of other factors, such as dependence on government officials or the use of intermediaries for government liaising may result in significant regulator scrutiny if not adequately addressed with proportionate procedures.

It is equally important to remember that doing business in countries with a demonstrable history of bribery and official corruption can have separate consequences for a company's business that potentially warrant disclosure.

Issues to consider include:

- Ensuring compliance with relevant local laws. In many cases, corruption spawned from the existence of overly bureaucratized legal and political institutions that lack proper oversight or, alternatively, gaps in the rule of law that make it difficult to ensure compliance. In such circumstances, it becomes all too easy for officials to seek bribes or other forms of compensation as a means of easing regulatory approvals or securing necessary contracts with official bodies.
- The presence of an endemic culture of corruption and bad governance in a country has consequences for its overall political stability. As noted below, civil unrest can be caused by a host of factors. However, one of the most prevalent is the perceived lack of economic opportunity in places where corruption is rife and in which only those connected to a ruling party or family are seen to benefit from economic development. Companies doing business in such countries may be fully compliant with all relevant anti-bribery and corruption laws but may, nonetheless, find their business impacted by political instability or other consequences of that corruption.

Many of these issues will come as no surprise to businesses that have been managing their compliance obligations for years. Increased public and regulatory focus on the issue, including prosecutions by jurisdictions outside of the United States, creates a unique set of circumstances for companies to consider as they reevaluate this risk area in the context of their capital raising activities.

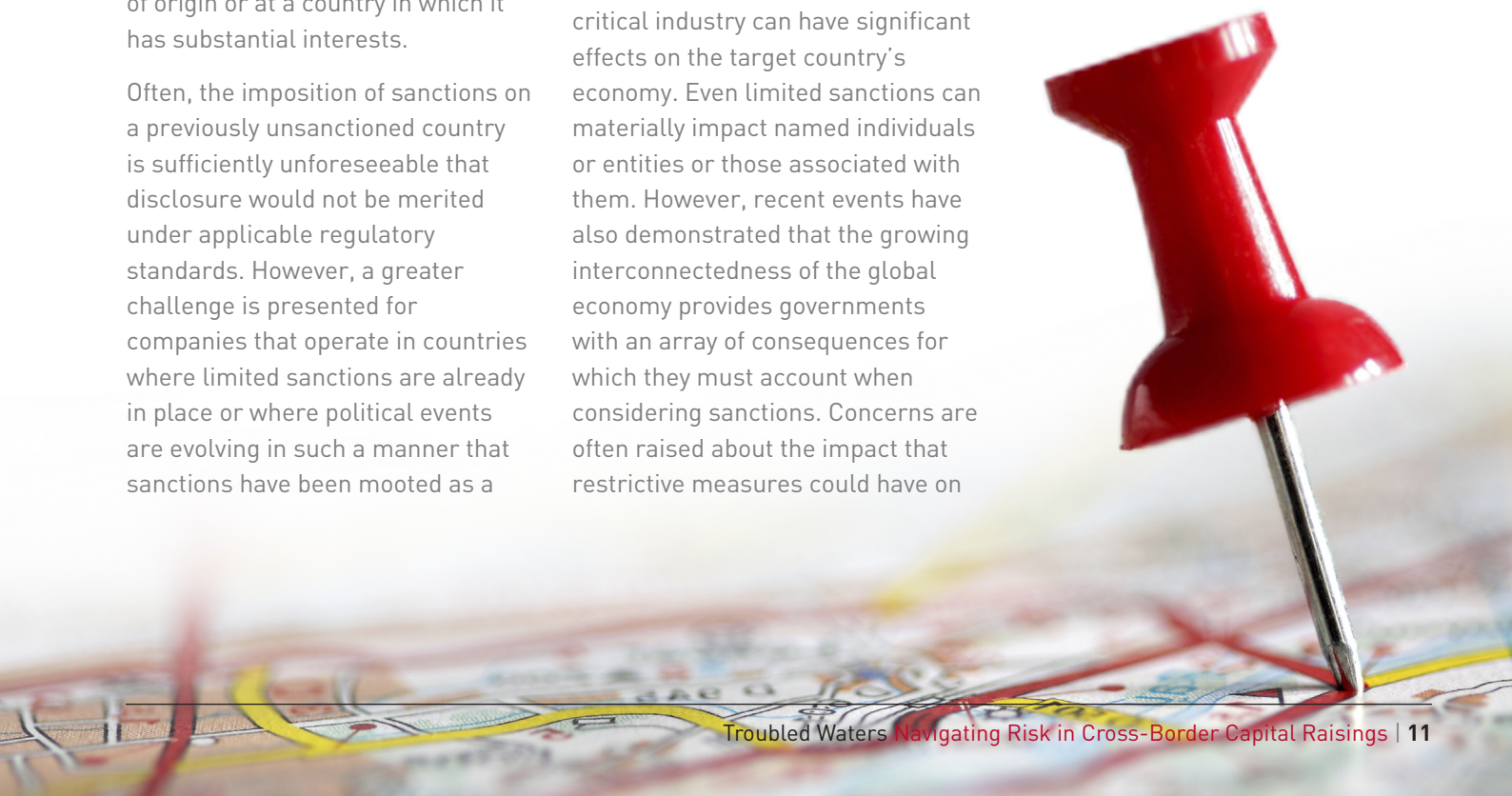
Trade Sanctions

As is the case with bribery and corruption compliance, companies doing business in foreign countries recognize the need to ensure that their activities do not contravene the complex web of trade sanctions, export controls, and embargoes in place at any particular time. Imposed either unilaterally by a particular country or by multinational bodies such as the European Union or the United Nations, such measures adopt a wide variety of forms and characteristics. Some sanctions apply only to transactions with a designated list of named individuals and entities, while others apply uniformly to all trade with a specific country. In addition to those that have been in place for decades, a range of more recent measures has been introduced, highlighting the dynamic nature of the landscape that businesses must navigate.

Working with local counsel, a company can audit its compliance with existing sanctions and determine with relative ease whether any related disclosures are necessary. The more challenging issue, from a disclosure perspective, will be for an issuer to consider whether its financial performance could, with reasonable foreseeability, be materially impacted by future sanctions aimed either at its country of origin or at a country in which it has substantial interests.

Often, the imposition of sanctions on a previously unsanctioned country is sufficiently unforeseeable that disclosure would not be merited under applicable regulatory standards. However, a greater challenge is presented for companies that operate in countries where limited sanctions are already in place or where political events are evolving in such a manner that sanctions have been mooted as a possible policy response. In those circumstances, it is necessary to assess the political circumstances in greater detail to determine the likelihood of a company's business or investment being affected.

On the one hand, the globalization of economic activity has made sanctions much more potent, given the increased value of cross-border trade and foreign investment. The imposition of sanctions on a critical industry can have significant effects on the target country's economy. Even limited sanctions can materially impact named individuals or entities or those associated with them. However, recent events have also demonstrated that the growing interconnectedness of the global economy provides governments with an array of consequences for which they must account when considering sanctions. Concerns are often raised about the impact that restrictive measures could have on



the imposing country's business community, for example. There are a number of circumstances in which such concerns ultimately outweigh the political imperative to punish a country for its behavior in the international political arena. Issuers should pay close attention to such dynamics when assessing the likelihood of sanctions impacting their business.

Equally, much as companies will consider the corruption-related implications of doing business with close associates of government officials, they should also consider the related complications from the perspective of sanctions. These measures frequently focus on taking punitive action against both key government officials and those who are connected to them. Companies should assess the extent to which their local business partnerships could become targets for such actions. In many circumstances, these lists of designated parties evolve over time, and such measures will often remain in place even as countrywide sanctions are lifted (as in the recent case of Myanmar). Accordingly, companies should closely monitor changes to such lists and consider the full consequences for their own business interests of any shifts in an imposing body's focus.

Even the imposition of limited sanctions can have a consequential impact on a targeted country's economy. Financial institutions could, for instance, curtail lending to companies based in sanctioned countries and foreign companies may suspend investment amid concerns that restrictions on trade could expand further to target a broader range of activities.

Finally, companies may find themselves attracting criticism from activists or non-governmental organizations that are calling for the imposition or expansion of sanctions on a particular country. Not only will targeted criticism generate associational risks, but calls for sanctions can also be tied to broader Corporate Social Responsibility scrutiny and compliance (as discussed on pages 22 and 23). Companies assessing sanctions as part of their disclosure process should consider their exposure to these types of issues as part of their overall assessment.

Opinions are divided on the actual degree to which economic sanctions can influence a country's foreign policy decisions. However, for the foreseeable future, they remain one of the most readily available policy tools with which to coerce change in the behavior of foreign governments. By their very nature, sanctions make multinational companies critical actors in their implementation, despite having little control over their imposition. Businesses should routinely assess the ways in which changes in existing sanctions or the introduction of new ones can or will affect their future interests.

Case in Point: Trade Sanctions

Events in 2014 in Russia and Ukraine combined to renew interest in the use of financial and trade sanctions as foreign policy tools.

Sanctions were imposed on a number of key members and associates of the government of former Ukrainian president Viktor Yanukovych in an effort to forestall the looting of state assets following his removal from power.

However, Canada, the United States, Japan, and the European Union also sanctioned Russian officials and entities following Russia's annexation of Crimea. The lists of designated individuals have expanded to include certain Russian business leaders considered close to the Kremlin and some financial institutions. As the conflict continued in eastern Ukraine in the summer of 2014, more extensive sanctions were imposed. These included measures to prevent specified Russian companies from raising funds on Western capital markets.

Some groups have called for sanctions to expand further and have criticized foreign companies that continued to do business with Russia.

This situation makes apparent the growing attractiveness of sanctions as a policy response to geopolitical challenges.

Domestic and Regional Political Rivalries

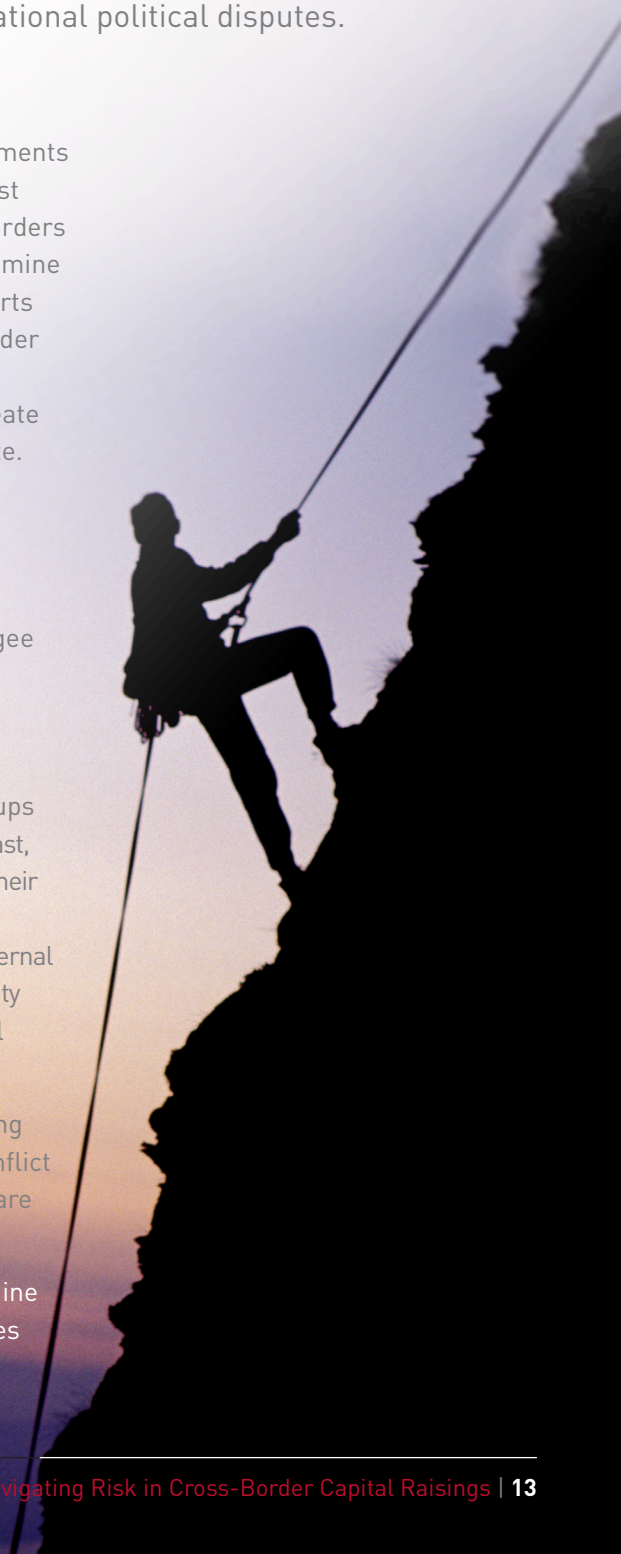
Geopolitical features characterizing high-growth, emerging or frontier markets are often considerably different from those encountered by businesses operating in more developed economies. In many such markets, it is a challenge to evaluate the ways in which unique geopolitical issues impact both the commercial environment as a whole and the activities of specific companies. Arguably, the best example of such an issue, one that is as opaque as it is potentially disruptive for businesses, is the existence of both regional and sub-national political disputes.

The most readily apparent of these disputes are those between governments and/or communities in neighboring countries. As a result, even the most diligent risk analysis might prove insufficient if its focus stops at the borders of the country in which a company does business and does not also examine potential challenges originating elsewhere across a region. In many parts of the world, most notably Africa, potential risks have their roots in border disputes that have never been addressed. But whether a dispute has these deeply embedded roots or has emerged more recently, it can create significant uncertainties in the environment in which companies operate.

There are three principal ways in which political rivalries can amplify companies' risk exposure:

- First, there is the potential for open hostilities to erupt between neighboring states. Such an event and its consequent effects – refugee crises, imposition of temporary military rule, and deterioration of transport links, among others – can all have significant impact on businesses' operations.
- Second, governments might lend support to opposition or rebel groups across their borders. In certain regions, especially Africa and the Middle East, governments sometimes seek to bolster their relative influence vis-à-vis their neighbors by lending discreet or covert support to groups fighting against regimes in those countries. Such support can transform a manageable internal security risk into a major crisis, and the resulting degradation of the security environment can have as great an impact on companies' operational capacity as that associated with open warfare between states.
- Third, tribal or ethnic conflicts can straddle borders. Because existing political boundaries often do not reflect demographic realities, a conflict in one country can spread across borders that divide groups that share tribal or ethnic identities.

Thus, risks that arise in one country must often be evaluated to determine the potential for spillover that could increase the exposure of companies operating entirely in another country.



However, even in places where regional tensions do not factor, political rivalries *within* a given country can prove equally troublesome, though often in ways that are more difficult to predict. At this sub-national level, disputes are most likely to take one of two forms:

- Rivalry between political elites. In markets characterized by immature political institutions, gaining power often means gaining access to a range of tangential perks. As a result, political disputes are often fierce, can sometimes be violent, and can thus impact companies perceived as too closely aligned with particular figures or parties if power subsequently changes hands.
- Disputes between sub-national demographic groups. Particularly in places where the economic benefits of foreign investment are not distributed uniformly among various communities, conflict can emerge that pits groups against each other over access to tax or royalty revenue, jobs, and other benefits that each claims as its right, creating challenges for companies caught in the middle of such disputes.

The space between the political and commercial spheres in a market often appears much greater than it is in reality. These disputes can substantially alter the conditions under which businesses operate and as a result are vital to understand.

The outbreak of conflict in a particular country can dramatically distort the local market for companies selling products there, leading to price volatility and making revenue projections uncertain. But even companies that are not directly affected by conflict-driven market fluctuations can often not escape the more general effects of political disputes. Governments that routinely perceive regional political influence as a sort of zero-sum game are likely to see regional economics through the same lens. Just as a national or sub-national government might seek to undermine the political power of its neighbors in order to boost its own, it might also aim to interfere with economic growth, under the false but common belief that such a move will enhance its own economic standing. It will be difficult for companies operating in a region marked by such circumstances to avoid any adverse impact on their profitability, and the resulting uncertainty can make this a risk that warrants disclosure.

Ultimately, this risk is important to understand and monitor because of its inherent uncertainty. It is difficult for outside observers of these disputes to be fully aware of their details. But it is crucial to seek an awareness and appreciation of them in the context of local circumstances and histories.

Case in Point: Domestic and Regional Political Rivalries

In Nigeria, a confluence of factors combine to create a complex web of domestic political rivalries, including the presence of hundreds of ethnic groups among the population, a strong bifurcation between the mainly Muslim north and the predominantly Christian south, and an uneven distribution of natural resources. The oil industry is particularly vulnerable to being caught up in these disputes that are largely opaque to observers beyond Nigeria's borders.

In August 2012, Nigeria's federal government declared Anambra state as the country's tenth oil-producing state. The move, based on a potentially lucrative oil discovery, is important because under current derivation laws, the designation allows the state to retain 13 percent of taxes on oil produced there.

Borders in Nigeria are often poorly demarcated, however, and neighboring Kogi and Enugu states appealed the decision and Anambra's ownership of the land containing the potential oil reserves. The dispute escalated in April 2013 amid reports that members of a Kogi community attacked residents of Anambra state in the vicinity of a disputed oil well in an incident that allegedly left multiple people dead.

There is a risk that foreign companies, on whose technological expertise Nigeria's oil production is dependent, can be caught up in such local political disputes and could face consequent legal, financial, and reputational impact.

Civil Unrest

On the surface, the relationship between societal and economic stability is clear in its general form – increased unrest almost invariably inhibits commercial activity. But the material effect that unrest will have on a company's profitability is less easy to determine. Risk exposure depends on a wide array of local and specific factors, including, among others:

- the industry in question;
- whether unrest is spontaneous or reflective of deep and long-standing grievances; and
- the nature of a government's response.

To understand the risks associated with civil unrest, companies must be aware of the various ways in which an erosion of political stability can impact their operations and interests.

The challenges presented are most acute in cases where an outbreak of unrest is driven largely by economic grievances. Under such circumstances, companies can find themselves criticized on two fronts: by a restive population that accuses private enterprises of doing too little to provide economic opportunity, and by governments anxious to deflect public anger away from themselves. This latter criticism can also serve as a precursor to steps designed to assuage popular sentiment, from implementation of windfall taxes to outright expropriation.

But even for companies not exposed to direct risks from civil unrest, the impact on financial or operational health can be real. Civil unrest depresses a country's economic prospects. This is apparent first in the short term as local market forces change in often unpredictable ways. But if periods of unrest linger and long-term political stability is threatened, even more substantial and enduring effects can be felt. Sustained unrest discourages prospective investors from injecting new capital, for instance, which further constrains economic growth and means that the repercussions will be felt even by those who are already invested in the country.

An outbreak of unrest in a country does not necessarily cause a measurable change in the risk profile of companies operating there. The key for businesses is to appreciate those qualitative aspects of unrest that define the magnitude of any resulting risks. In order to accurately assess their exposure, they must consider a variety of factors, including:

- Underlying dynamics driving unrest. If economic considerations like high unemployment levels or severe wealth gaps represent the principal causes of public anger, unrest is more likely to affect businesses because of the likelihood that they are seen to contribute to the problem. But even if public grievances are not economic in nature, identifying and evaluating their causes will offer important indicators of a company's risk exposure. If unrest is generated in response to a single, explosive event, for example, a rapid and adequate government response often defuses a combustible situation quickly. Similarly, if anger is directed at particular leaders or a specific political party, certain steps such as holding new elections or concluding a power-sharing arrangement can calm angry popular sentiment. But if civil unrest represents a boiling over of a long-standing or deep-seated sense of injustice, both the period of unrest and the risks confronting businesses are more likely to extend over a longer period.

- Geography of unrest. In the past, political protest and anti-government activity were often confined to specific pockets within a country, typically capital cities, major commercial centers, and other urban areas. But transformations in the media sphere have eroded this predictability. The Internet changed the pattern to a considerable degree, and the advent of social media tools has done so even further. Yet unrest continues to manifest itself unevenly in countries perceived as most completely wracked by the chaos of widespread popular protest. Geographic patterns are fluid and changes can be abrupt, but they also leave companies in different areas of a troubled country or region facing very different levels of risk.

- Government response to unrest. Regimes can react in a number of ways to the emergence of civil unrest. Governments that feel their survival threatened, for instance, are likely to act most forcefully. But while their response might be troublingly aggressive, it is also more predictable than that of governments that feel themselves less fundamentally vulnerable. Other factors also influence this response. Situations in which the regime or key officials have a considerable stake in the economy, for instance, are most likely to see the government weigh the impact of their actions on the economy and business environment. These and other determinants of a formal response by the state will play a role in shaping the risk exposure that companies face.

Preparing to face risks associated with civil unrest and forecasting their potential impact on financial performance requires three steps. Companies must:

- dispassionately evaluate the objective likelihood that unrest will occur;
- assess a range of factors that combine to determine their particular risk exposure; and most importantly,
- seek to mitigate such risk by positioning themselves as part of a solution to the issues that drive unrest and contribute to instability, rather than letting themselves be perceived as part of the problem.

Case in Point: Civil Unrest

In December 2007, general elections in Kenya saw the country's incumbent president re-elected. Widespread allegations of fraud followed, as did mass protests across the country by people heeding the call of opposition leaders to take to the streets. The protests quickly devolved into a period marked by clashes between protesters and security forces, as well as sectarian violence. The unrest lasted two months, claiming the lives of hundreds and displacing tens of thousands.

During the unrest, the economy virtually ground to a halt. At the local level, return to normal economic activity posed an immense challenge, as many small and mid-sized companies saw buildings torched and infrastructure destroyed, and the Kenyan government lacked the resources and did not have the institutional mechanisms in place to facilitate rapid rebuilding. More broadly, the country's growth also suffered, with billions of dollars worth of economic activity lost. The tourism sector was particularly hard hit, with revenues during and in the months after the unrest down nearly 80 percent over the previous year.

In many ways, Kenya was, and remains, one of the better functioning and more stable states in sub-Saharan Africa, and has thus been an attractive destination for foreign capital. Nevertheless, the combustibility that resulted when a match was struck – in this case, disputed elections – offers an instructive lesson about the importance of assessing dynamics that lie just below the surface layer of stability.

Resource Nationalism

In some cases, political and security-related risks will impact companies and industries uniformly. But many others will be unique to a particular sector. The most readily apparent example of the latter is the periodic resurgence of the phenomenon of "resource nationalism."

In recent years, strong global demand for many natural resources has yielded considerable financial rewards for companies extracting, refining, and marketing them. However, such sustained profitability has also given rise to a political debate in many resource-rich countries about whether a sufficient share of revenue from extractive industries is being captured for the benefit of local populations. This has prompted governments in both developing *and* developed countries to institute policies aimed at redirecting income from resources companies to government treasuries.

Even as demand for many resources is forecast to slow over the next few years, the political imperative to redefine relationships with private resources companies will likely remain. In fact, as reduced demand pushes state revenues downward, even further pressures on governments to act in this regard could emerge.

In its most overt form, resource nationalism involves the outright expropriation of assets by a government. Worldwide trends in this behavior have waxed and waned historically. However, even when cases of full-scale nationalization are limited, as they have been in recent years, the risk is never fully removed from the global economic and political landscape. In 2012, for example, the Argentine government partially renationalized the energy company YPF from its Spanish owners. Former president Hugo Chavez of Venezuela undertook a number of similar actions over the past decade affecting a range of industries, including oil and gas exploration and production.

This sort of full-scale expropriation can reverberate in negative ways for governments, hence its infrequent occurrence. Companies from many countries rely on bilateral investment treaties to safeguard their assets against expropriation. Even if this is not the case, they will often litigate to recover losses suffered. The elasticity of foreign investment also means that few governments are prepared to risk the damage to their country's investment reputation that comes with a decision to nationalize the assets of a certain company or industry.

Nevertheless, the risk of nationalization has not disappeared completely. Where governments are confronted with significant domestic political, social, and economic challenges, nationalization can appear to be a panacea. Companies should pay close attention to the political rhetoric about issues such as foreign ownership and control of natural resources in countries where they operate.

Case in Point: Resource Nationalism

Over the past decade, Mongolia saw an influx of investment from foreign resource companies seeking to develop its substantial mineral resources. In time, however, some of its political leaders expressed concerns that the country's people were not benefiting sufficiently from that boom.

Following parliamentary elections in 2012, efforts to redefine the terms under which foreign companies operated in Mongolia came under greater scrutiny. New laws were introduced requiring government approval for new investment in strategic economic sectors such as mining. The government also sought to reopen royalty sharing agreements with existing investors.

This combination of events resulted in a substantial decline in new investment activity in the country and some existing investors threatened to suspend business rather than submit to renegotiation of royalty agreements. The Mongolian government eventually rescinded many of the new restrictions, but investors continue to pay close attention to the political debate over approaches to foreign investment in the country.

However, in the vast majority of cases, efforts by governments to assert greater control over their natural resources sectors take less overt forms. And despite their subtlety, such measures pose challenges to the viability of foreign businesses. Recent years have seen examples of governments:

- unilaterally reopening previously agreed royalty or taxation agreements with resources companies and demanding new terms that are more favorable to national treasuries;
- strengthening indigenization laws requiring either local participation in new projects or partial sales of existing ownership back to members of the local population;
- enacting "mandated beneficiation" laws requiring activities such as processing of raw materials to be performed in-country, rather than exporting them for refining elsewhere; and
- making incremental changes in regulatory and business environments that, collectively, encourage foreign investors to exit the country and, when combined with legal restrictions requiring sales of existing investments to local companies, have the desired effect of bringing industries under domestic control.

Cumulatively, then, even seemingly minor regulatory changes can fundamentally alter the environment in which resources companies operate. Companies should remain mindful of individual local changes and developments that might indicate that a government is pursuing a policy program that effectively amounts to resource nationalism.

Moreover, such trends can be driven by forces that are much more complex than a simple desire to retain or regain control of a strategic industry for local companies or investors. As noted above with respect to civil unrest, long-standing historic or cultural tensions in a particular country can influence popular attitudes to foreign investment and create a political imperative for asserting greater control over sectors that are seen as critical to a national economy.

By assessing a country's evolving legal and regulatory environment in the context of local political and economic conditions, companies will gain a better understanding of the reasons for policy changes. They will also be better equipped to evaluate long-term implications on the viability of their investments and commercial interests.

Terrorism

Terrorism is unique among risks facing businesses in that, by nature, it can manifest itself in violent and damaging fashion nearly anywhere in the world. It is also arguably the most direct security risk that companies confront when doing business in markets of uncertain stability. Its dangers are especially acute for those operating in areas with distinct, established terrorist threats.

Terrorist attacks remain rare, despite their propensity to attract disproportionate media attention. And it is important to keep this rarity in mind. Companies must strike a balance between being prepared for a highly unlikely event and ensuring that preventive measures are commensurate with the level of risk faced. Protective measures can impact a business' operational and financial health. However, because of its innate unpredictability, terrorism remains a paramount risk for businesses to appreciate.

Terrorism can principally impact companies' interests by directly threatening the safety of their personnel and the security of their property and infrastructure. But in order to fully appreciate potential threats, it is critical to understand that attacks against companies are not always intended as ends in themselves, although they can be. Often, they are designed as means to an end that has little to do with the business victimized by an attack.

When a terrorist group chooses to directly target a company, this choice is intended to send a message. Terrorism, to a greater extent than almost any other form of conflict-related violence, is designed as a form of communication. Without this element, terrorist violence is indistinguishable from that of criminal organizations. Target selection is key. Foreign companies, or even those perceived as such, can appear as attractive targets.

But businesses can be vulnerable to attacks motivated by other considerations, too – those in which the attack itself serves a more fundamental purpose. The clearest example of this is when hostages are taken and held for ransom, and the resources available to large companies make their personnel among the most appealing targets for such an attack.

Companies might also find themselves targeted because the industry in which they operate is vital to a country's economy. Terrorist organizations are often motivated to demonstrate their ability to harm a government where it is vulnerable. A country whose economy is heavily dependent on revenues from the tourism sector or natural resource extraction, for example, can sometimes see a heightened threat to companies in those industries. While businesses might serve only as indirect targets in attacks aimed primarily at harming a government's interests, the resulting damage will be no less severe.

In either case, whether a business represents a terrorist group's

Case in Point: Terrorism

In January 2013, a large force of Islamist militants forced entry into a natural gas facility situated deep in the desert of Algeria, near the border with Libya. The fighters killed a number of foreign workers and took others hostage. Algerian security forces responded aggressively, and by the end of the subsequent battle, dozens had been left dead.

The facility was operated as a joint venture between Algeria's state-owned firm and two European companies. The militants deliberately targeted foreigners, but the nationality of the victims was not apparently important, despite the statement by the group responsible for the attack that it was undertaken in response to France's military intervention in neighboring Mali. Thus, the country in which a company is based has little measurable effect on its relative risk vulnerability.

Militant groups often deliberately refuse to distinguish between governments and private companies when conducting attacks. As a result, it is critical for firms to be vigilant and regularly monitor a broad array of geopolitical trends, as well as the shifting dynamics of popular sentiment in the regions where they operate, even as it relates to issues that do not specifically involve their activities.

direct or indirect target, preventive measures substantially reduce risk exposure. Among these measures are appropriate personnel and infrastructure security and a commitment to maintaining a low profile where possible. But equally, companies must be prepared to respond to any attack. A rigorous and systematic crisis management program is vital, as is insurance coverage that specifically covers losses resulting from acts of terrorism. These measures are discussed further in Section Three.

It is also important to note that companies can be affected not only by the risk of terrorism, but by steps taken by local governments to counter the threat. Regimes that feel their political control threatened by terrorist organizations will often resort to aggressive measures to protect their hold on authority. In countries where the rule of law is less deeply established, these actions might generate considerable condemnation from the international community. As a result, a second-order risk arises whereby the physical security threats associated with terrorism are less acute than the reputational risks of doing business in a country where respect for human rights is subordinated to a regime's survival instinct. This is particularly the case in countries where the state's active involvement in the economy contributes to a view that doing business *in a country* is synonymous with doing business *with the government*. This issue is considered further in the discussion on associational risk above.

Ultimately, being prepared for the risk of terrorism requires an acceptance of its unpredictable nature and a flexible approach capable of identifying signs that indicate potential changes in a company's exposure to the threat. In order to determine the extent to which terrorism presents a material risk that warrants disclosure, managers should seek a comprehensive understanding of the local nature of this global threat, and should be aware of the measures available to mitigate risks associated with it.

Cyber Threats

Cyber threats are unique among political and security risk factors in that a company's vulnerability to them is least likely to be a function of the political and security environment in countries where it operates. More than any other risk factor discussed here, cyber threats are truly transnational in character.

Threats in the cyber domain are also the newest that companies in the private sector face, and are by far the most rapidly evolving. These two factors combine to leave businesses perpetually less sufficiently prepared to mitigate the risk of cyber attack or network disruption than they are for those risk areas with which they have been confronted over a longer time or that are comparatively more static in nature. Yet protecting against cyber threats is essential, not only because of the potential for financial loss or operational disruption, but also because of a growing view among regulators that a company's exposure to such threats should be more adequately and formally disclosed.

Several factors contribute to determine the vulnerability of a company's networks. While businesses can suffer from blanket cyber threats that do not target them directly, the most acute danger arises when an enterprise is deliberately targeted. This can occur as a result of several factors, but is most typically a function either of the industry in which a company conducts its business or of its specific operational decisions and policies.

Like many security-related challenges, the risk of cyber threats is one in which both the technologies employed by assailants and those available to defend against attacks are evolving rapidly and in response to one another. The cyber risk environment is in a constant state of flux, marked by a perpetual cycle of exploitation of weaknesses and efforts to secure points of vulnerability.

Cyber threats can take a number of forms that are potentially harmful to businesses, but two in particular need to be understood in detail:

- **Information theft**. Business espionage is not a new feature of the global economy. For years, some companies have undertaken efforts to overcome competitive disadvantages by stealing proprietary information from their competitors. But as businesses increasingly rely on technology to store and manage vast quantities of information, this threat has transformed. The growth in scale of state-owned enterprises (SOEs) that has turned many of them into competitors of multinational companies with no government affiliation has further amplified this challenge. New technologies developed and employed by government intelligence and security agencies can be harnessed by SOEs, heightening the vulnerability of businesses in highly competitive global industries.
- **Network disruption**. Incidents such as denial-of-service (DoS) attacks are conducted with the intent of rendering a target's computer networks unresponsive and thus unable to support ongoing business operations. Unlike cyber theft, disruptive attacks are not typically motivated by a desire for competitive advantage. Rather, they are more likely to be undertaken by activists whose agenda pits them against companies operating in particular industries. Natural resource companies have been attacked in the past, but a wave of anti-corporate sentiment in the wake of the recent global financial crisis has left companies across a range of sectors victimized.

Besides its novelty and rapid evolution, the risk of cyber threats is differentiated by a further characteristic from other risk factors discussed here. Unlike terrorism, civil unrest, or issues of resource nationalism, measures taken to protect against cyber threats must be almost wholly technological. While adopting an appropriate security posture can limit a company's vulnerability to terrorist attack and working with various stakeholders can mitigate against potential damage associated with political instability, little can be done to change the fact that both competitors and ideological activists will target businesses in the cyber domain. Instead of taking steps to reduce the scale of the risk, companies must focus instead on reducing their vulnerability by developing robust protective measures.

It is vital for companies to be fully aware of the extent of their exposure to cyber threats. And given the complex issues associated with cyber security, companies must be able to demonstrate their commitment to protecting themselves not only to shareholders and customers, but also to regulators that are increasingly likely to require disclosure of both risk exposure and security measures in the cyber domain.

Corporate Social Responsibility

Although the term was first coined decades ago, companies have found themselves under growing pressure in recent years to demonstrate their commitment to corporate social responsibility (CSR). The term has extremely broad application, but it revolves around the concept that companies should pair profit maximization with efforts to be good "corporate citizens." CSR can encompass an array of issues ranging from the use of conflict minerals to environmental practices but, given its broad nature, has spawned a number of new initiatives over time.

The legal approach to encouraging CSR among companies varies from country to country. Some governments have focused on encouraging subscription to voluntary codes of practice on various CSR-related issues, while others have imposed mandatory obligations on companies to implement specific initiatives. Advocates of CSR measures are increasingly looking at capital markets and their mandatory disclosure rules as a mechanism through which effective CSR reporting can be encouraged. Some governments have already taken up such initiatives and introduced requirements for CSR-related disclosures. These range from obligations to make general disclosures about a company's overall CSR efforts to requirements to make particular disclosures about a company's use of specific products, such as conflict minerals, in its supply chain.

To date, the United States Securities & Exchange Commission (SEC) has not adopted rules requiring companies subject to its jurisdiction to make broad CSR-related disclosures, although a number of European countries have implemented such requirements. The SEC has, however, implemented disclosure rules in relation to a number of issues that would fall under the umbrella of CSR. In other cases, companies are considering whether disclosures on some CSR-related issues should be made under general reporting requirements. Three of these issue areas have garnered particular attention and require special consideration by companies: environmental sustainability and climate change, conflict minerals, and compliance with anti-bribery and corruption laws such as the Foreign Corrupt Practices Act, each of which is considered elsewhere in this publication.

Nevertheless, the possibility remains that further new measures will be introduced, since political momentum exists in many countries to make CSR compliance mandatory, rather than simply voluntary. Moreover, many of these initiatives are likely to involve issues relating to companies' international business operations, given the particular sensitivities that exist about corporate behavior in developing economies. Companies with comprehensive knowledge of

Case in Point: Corporate Social Responsibility

In the wake of labor unrest in the South African mining industry in 2012, certain mining companies announced financial losses that caused them to contemplate cost-cutting measures. These included redundancies and closure of underperforming mines.

The announcement of these measures attracted criticism from South African politicians, with at least one government minister calling for companies that proceeded with such redundancies to lose their remaining operating licenses.

Compromise solutions were eventually agreed, but the situation highlights that the process of balancing the interests of company profitability with the interests of other stakeholders can often have political implications. Coming at a time when South Africa was experiencing relatively high unemployment, these decisions involving mass redundancies placed the companies involved in politically precarious circumstances.

the local political environment in countries where they do business will be better placed to assess how their business may be impacted by particular CSR initiatives.

As an example of this move toward greater regulation of CSR-linked issues, in 2013 the United States government enacted regulations under which any US person or entity is required to report any new investment in Myanmar valued at over USD500,000 or any investment of any value in that country's oil and gas industry. These reporting rules were introduced after the US and other Western governments opted to lift sanctions barring investment in Myanmar in response to political reforms enacted by its government. The new reporting requirements are intended to serve as a means of allowing both official and public scrutiny of new investment activity and of encouraging US companies to invest in ways that will promote the country's further political and economic reforms.

Given the fluid nature of attitudes and policies with respect to CSR, reporting requirements related to these issues will continue to evolve over time. Companies seeking to raise finance on international capital markets should seek the advice of local counsel on country- and industry-specific initiatives that could be applicable at any point in time.

Conflict Minerals

Since 2009, attention from regulators to the production, sale, and use of so-called "conflict minerals" has grown substantially. At its most general level, the term refers to any mineral resources extracted in regions where armed conflict is occurring. However, for disclosure and regulatory purposes, the term currently refers to a specific group of mineral ores mined in eastern parts of the Democratic Republic of Congo (DRC) and neighboring countries. Serious human rights abuses in this region have been linked to mining activity and revenues from mineral sales have funded local insurgent groups, thereby prolonging regional political instability.

Sustained pressure to confront this problem led the US Congress to include provisions in the Dodd-Frank Act of 2010 requiring companies to disclose their use of designated conflict minerals in manufacturing processes. The aim of the legislation was to draw attention to companies that use such minerals and, thereby, create public pressure for them to curtail doing so. The disclosure requirements apply to any company that manufactures products where "conflict minerals are necessary to the functionality or production of the product" and covers both US and foreign companies that have issued securities subject to the jurisdiction of the SEC.

The materials that constitute "conflict minerals" are designated by law and can be amended from time to time. At present, the designation refers to a specific list of minerals extracted in a set of defined "Covered Countries." The minerals are as follows:

- Cassiterite: the principal ore used in the production of tin;
- Columbite–tantalite: the ore from which tantalum is extracted, for use in the production of electrical components, tool parts, aircraft engine components, and a range of other industrial products;
- Gold; and
- Wolframite: an important component in the production of tungsten.

Currently, the "Covered Countries" are Angola, Burundi, the Central African Republic, the DRC, Rwanda, the Republic of Congo, South Sudan, Tanzania, Uganda, and Zambia.

The SEC has issued detailed guidelines on how disclosure requirements will be implemented and enforced. Draft versions of these guidelines, published in late 2010, prompted considerable comment about their practicality. Following the failure of a court challenge questioning the provisions' legality, affected companies were required to make their first report in 2014.

The increased overall attention being paid to conflict minerals and to the substantial compliance requirements they raise requires consideration of a number of broad issues. These are important not only for mining companies, but also for those in a wide range of industries whose operations might be scrutinized for connection to conflict minerals, even if they are not currently caught by the applicability of the US legal provisions. They are as follows:

- The complex nature of the smelting and manufacturing processes connected with the use of conflict minerals in many companies' supply chains means that compliance auditing will likely prove extremely complicated. Many companies now anticipate that they will be unable to declare themselves "conflict-free" – at least for early reporting periods. Accordingly, consideration should be given to both the potential legal and reputational consequences of such a situation and appropriate disclosures made where necessary.
- The European Union published draft regulations on conflict minerals in 2014. The scope of these EU rules differs in a number of ways from the US equivalents. When enacted, these measures will affect a large tranche of companies not covered by the SEC guidelines and their final terms will need to be considered closely.
- The overall political situation in parts of sub-Saharan Africa where conflict minerals are sourced remains highly dynamic. New armed groups or regional conflicts emerge routinely, giving rise to new potential sources of supply risk and impacting the supply chain due diligence that companies will be conducting. Control of territory by governments sub-Saharan Africa is highly fluid, with potentially safe mining regions at risk of falling into rebel hands. This occurred in 2012 when M23 rebels in the DRC temporarily seized the resource-rich territory in the country's east. Accordingly, companies whose business may involve the use of conflict minerals should assess current political and security situations in affected countries in order to ensure that their disclosure and compliance obligations are as accurate and up-to-date as possible.

The issue of conflict minerals continues to evolve, in terms of both how companies respond to new reporting requirements and how regulators deal with pressures to expand reporting requirements to other countries and other materials. Knowledge of the underlying political dynamics will help companies fulfill their reporting obligations and anticipate further challenges.

Case in Point: Conflict Minerals

The introduction of mandatory reporting requirements for use of conflict minerals caused many companies to undertake extensive due diligence on their supply chains. In a number of cases, this exercise confirmed significant difficulties in tracking the provenance of minerals from their mine of origin through the production process.

Concerns about satisfying SEC compliance requirements have led a number of companies to invest extensively in the past year or so in improving their capacity to track mineral use. In other cases, companies have announced that they will only source materials from regions like North America where they can carefully monitor extraction activities.

Companies that have taken such decisions acknowledge that this may result in increased costs in their production process. However, most contend that such costs are outweighed by the financial and reputational risks associated with use of conflict minerals or failing to disclose the same.

Climate Change and Sustainability

As with other issues that fall under the still relatively young rubric of CSR, disclosure requirements associated with climate change and sustainability remain highly fluid. As such, fulfilling them requires a dynamic approach and a commitment to monitoring the rapidly changing regulatory environments in a wide range of jurisdictions.

Unlike other CSR issues, including those discussed here, neither climate change nor sustainability is typically understood as a political risk. At their core, these are climatic, ecological, and social challenges. And yet the growing attention that these issues have garnered in both national capitals and international political bodies has led to increased political action to address them. A combination of ambitious, multinational programs and individual national regulatory undertakings has created a web of disclosure obligations with which companies must comply.

Climate change itself, as the SEC has noted, can have material operational and financial impacts across a range of industries. These potential effects are particularly acute for companies operating in markets where less developed political institutions and limited technological bases combine to form a regulatory environment where little has yet been done to combat an issue of intensifying global concern. But this is rapidly changing, and as a result, companies doing business in these countries should expect to see further compliance requirements introduced both by local authorities and those in the countries where they are based and where they raise financing on capital markets.

Political pressures have led to the introduction of disclosure requirements for companies in an array of sectors. Companies can be required to disclose the nature of climate-related legal and regulatory frameworks within which they will operate. They can also be expected to define the potential risks to operations and future financial performance associated with climate change, impacts of which potential investors will be eager to find out.

Growing public awareness of and political attention paid to the issue of sustainability have also changed the way in which companies must view their disclosure obligations. In some developing countries, governments are only now beginning to undertake to regulate companies operating there to ensure environmentally and socially sustainable operations. As a result, new regulatory changes can be frequent. Companies should pay close attention to the introduction of such changes and be prepared both to disclose and demonstrate compliance with them.

But financial performance will also be influenced by each company's image among the global public. A company's profitability will be enhanced if its operations are seen to be in line with the sentiments of its customer base, and consumer trends show consistent growth in the emphasis placed on sustainable business practices. Similarly, and in part a function of investors' recognition of the importance of sustainability for profitable companies, existing and potential investors will continue to pay considerable attention to disclosure documents that demonstrate a company's commitment not just to satisfying all relevant regulations, but to pursuing sustainability as an end in itself in order to promote long-term investment security.

Case in Point: Climate Change and Sustainability

Brazil has been at the forefront of a trend in Latin America toward imposing robust environmental and sustainability standards on companies operating in the country. As with other countries in the region, particular attention has been paid to the hydrocarbons industry.

Oil companies that are alleged to have caused not only environmental but also social damage have been the subject of lawsuits by Brazilian prosecutors. While these suits have sought to impose financial penalties, significantly, they have also included penalties that would shut down part or all of companies' operations.

But whereas companies in the oil, gas, and mining sectors have been among the most visible of those involved in high-profile and costly cases involving environmental laws around the world, Brazil has also held foreign companies in other sectors equally accountable. Beyond environmental sustainability issues, companies in a range of industries have been penalized for unfair business practices in rural areas and for engaging in activities seen to threaten traditional modes of living, for example.

Non-governmental organizations have been especially central to lobbying for stricter regulations and harsher penalties, and have been active in seeking to hold companies accountable to existing laws in Brazil. As the world continues to transition to one in which states are not the only actors who influence regulatory environments, particularly in developing markets, this is a trend that will spread well beyond Brazil and into countries across Latin America, and in Africa and Asia, where rapid economic growth is forecast in the years to come.

Concluding Summary

The global financial crisis has had a lasting impact on many aspects of the global economy and the international financial services industry. Not least of these is a renewed emphasis on the identification and mitigation of risk. As companies around the world return to international capital markets to raise capital, they are experiencing this renewed emphasis firsthand.

Nowhere is this greater focus on risk more apparent than in the disclosure process, and careful consideration of the risks that a company faces is essential to the successful management of that exercise. This includes anticipating changes in the issuer's operating environment. This publication has highlighted a number of the external factors that impact the political and security risk environments in the emerging markets that are attracting increasing interest, from investors and regulators alike.

Effective disclosure can not only limit exposure to the risks areas discussed here but, if done properly, can also help companies to satisfy the demands of investors for information that demonstrates an appreciation of risk and links it to the valuation of shares being offered for listing. The process can also serve as the basis of an ongoing risk management process. Finally, it is especially important to use advisors with strong local and international knowledge to gain a better understanding of how these challenges will impact both the issuer's business and its associated disclosure obligations.

About Baker McKenzie's Global Capital Markets Practice Group

Baker McKenzie's Global Capital Markets team comprises nearly 360 capital markets lawyers in more than 47 countries, including all of the world's leading financial centers. The Firm represents issuers and investment banks in a wide variety of IPOs, cross-border listings and other capital markets transactions, including debt, equity and equity-linked issues, and in complex, multi-jurisdictional acquisitions and divestitures involving public companies. Over the past five years, the Global Capital Markets team has been involved either as issuer's or underwriter's counsel in more than 530 equity and debt offerings, valued in total at approximately US$350b. The practice is consistently ranked among the top corporate law firms globally and in the world's largest capital markets.

Steering committee members

Pablo Berckholtz
Lima
+51 1 618 8500 x 508
pablo.berckholtz@bakermckenzie.com

Edward Bibko
London
+44 0 20 7919 1343
edward.bibko@bakermckenzie.com

Amar Budarapu
Dallas
+1 214 978 3060
amar.budarapu@bakermckenzie.com

Frank Castiglia
Sydney
+61 2 8922 5254
frank.castiglia@bakermckenzie.com

Ashok Lalwani
Singapore
+65 6434 2684
ashok.lalwani@bakermckenzie.com

Manuel Lorenz
Frankfurt
+49 0 69 29 908 606
manuel.lorenz@bakermckenzie.com

Thomas Rice
New York
+1 212 626 4412
thomas.rice@bakermckenzie.com

Erik Scheer
Amsterdam
+31 20 551 7538
erik.scheer@bakermckenzie.com

Koen Vanhaerents
Brussels
+32 2 639 36 11
koen.vanhaerents@bakermckenzie.com

About Global Torchlight

Global Torchlight is a dynamic and specialized consulting group advising clients on a full spectrum of international political and security issues.

The group was co-founded by John C. Amble, a former United States Army intelligence officer, and David J. Chmiel, a former cross-border mergers & acquisitions lawyer with one of the world's leading law firms. Capitalizing on a unique blend of training and professional experience in the private sector, government intelligence, and academia, we provide our clients with analysis of critical trends and developments in local political and security environments that impact directly on their business and investment decisions.

We work with clients in an array of industries and at every stage in the process of doing business in strategically important markets around the world. Our clients range from those considering a first-time investment in a new market to those with established interests who seek to better understand the relevance to their business and investments of emerging developments and evolving trends in a particular country or region. In addition, we are regularly sought out to provide expert commentary and opinion on global political and security risk developments in the British, Canadian, and U.S. print and broadcast media and in professional seminars and conferences on international business and investment matters.

www.bakermckenzie.com

Baker McKenzie has been global since inception. Being global is part of our DNA.

Our difference is the way we think, work and behave – we combine an instinctively global perspective with a genuinely multicultural approach, enabled by collaborative relationships and yielding practical, innovative advice. Serving our clients with more than 4,200 lawyers in more than 45 countries, we have a deep understanding of the culture of business the world over and are able to bring the talent and experience needed to navigate complexity across practices and borders with ease.