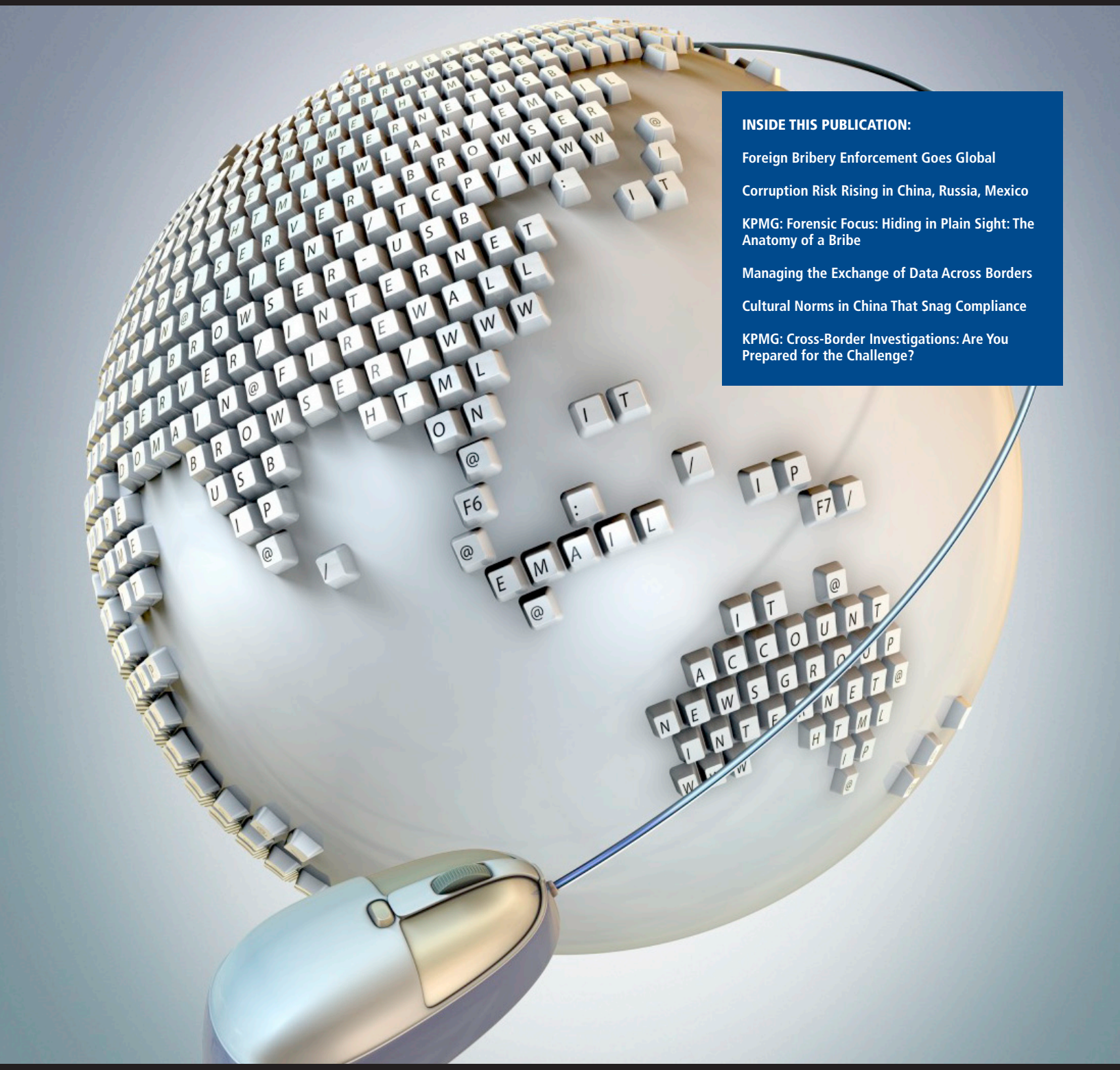
Brought to you by the publishers of COMPLIANCE WEEK



INSIDE THIS PUBLICATION:

Rising Global Corruption Risks and

Cross-Border Investigations

An e-Book publication sponsored by KPMG

It may be a small world, but bribery and corruption can bring big problems.

There are few boundaries to opportunity in the global marketplace. Unfortunately, the same is true for bribery and corruption—and the damage they can cause. In order to protect themselves, multinational organizations must have comprehensive anti-bribery and corruption programs in place. And that's where KPMG can help.

Through our global network of 2,500 forensic professionals, we offer a range of services to help prevent, detect and respond to corruption risks—and develop and maintain an effective compliance program. Because threats to your reputation—and success—are out there. And they don't stop at the border.

Learn more by visiting **kpmg.com/us/forensic**

KPMG
cutting through complexity

© 2013 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. 131113

Inside this e-Book:

COMPLIANCE WEEK

Compliance Week, published by Wilmington Group plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has quickly become one of the most important go-to resources for public companies; Compliance Week now reaches more than 26,000 financial, legal, audit, risk, and compliance executives.

KPMG works with organizations to help them in their efforts to achieve the highest level of integrity through the prevention, detection, and investigation of fraud and misconduct, and by avoiding and resolving disputes. At the same time, we work with businesses to effectively manage the costs and risks of complying with new regulations and enforcement activity and the dangers of disruptive litigation.

KPMG Forensic[SM] has a global team of more than 2,500 dedicated professionals from member firms. We have the necessary familiarity with domestic markets and foreign cultural standards, language skills, and local regulatory and privacy laws to consistently deliver high-quality results by leveraging KPMG's proprietary global investigation methodology.

KPMG's Investigation Services team works closely with clients to understand investigation objectives and coordinate our approach to utilize the appropriate resources. Through detailed inquiries and examinations, including the use of leading data analytic techniques, our highly credentialed professionals provide an impartial means to establish truths, evaluate implications, identify appropriate remedial actions, submit restatements if necessary and communicate with regulators or outside auditors if needed.

Through central coordination, our services are scalable—from a small team in one city to many teams operating simultaneously in dozens of countries. A single point of contact can readily assemble local or multinational teams to help ascertain the pertinent information so that a concern or situation can be swiftly resolved with minimal disruption and cost.

Professionals in our Forensic practice draw on extensive experience in law and regulatory enforcement, fraud and misconduct risk assessment, ethics and compliance program evaluation, asset tracing, forensic accounting, computer forensics, and forensic data analysis.

www.kpmg.com/us/forensic

Foreign Bribery Enforcement Goes Global

By Jaclyn Jaeger

Over the last several years, the United States has dwarfed all other countries on prosecuting cases of global corporate bribery and corruption. While no one expects that to change anytime soon, other countries are getting into the act and pursuing more foreign bribery cases of their own. That means companies may be forced to answer to multiple regulators in multiple countries, all with their own guidelines and investigation requirements.

In August, for example, Britain's Serious Fraud Office brought its first ever charges under the U.K. Bribery Act since the law's enactment in July 2011. The SFO brought charges against three executives and one financial adviser for conspiring to commit fraud by false representation and conspiring to furnish false information.

According to Paul Friedman, co-chair of the FCPA and anti-corruption task force at law firm Morrison and Foerster, the prosecution signals the "end of the quiet spell" pertaining to the SFO's lack of enforcement actions. "We're likely going to see more results as cases that are being developed come to a head," Friedman says. "We will certainly see charges brought against corporate entities in addition to individuals."

SFO Director David Green has publicly confirmed that two other investigations are pending against companies. "The SFO has always taken a robust approach to bribery and corruption, and we will continue to use the full range of tools at our disposal as befits the alleged conduct," says Jina Roe, press and information officer at the SFO.

"Most multinational companies have taken the Bribery Act very seriously," says Friedman. "This development reinforces the need to continue to do so, despite the relative lack of cases that have been brought since its enactment."

The United States continues to lead the way by far when it comes to enforcement of foreign bribery cases. Since 2002, the U.S. government has pursued 302 foreign bribery enforcement actions, according to anti-bribery group TRACE International. This figure represents eight times as many as the United Kingdom, which brought the second highest number of cases, with 38 enforcement actions, all of them corruption-related offenses brought under statutes other than the Bribery Act.

Northern Exposure

Canada has also taken significant steps in the anti-corruption area. "It's almost like the witching hour for anti-bribery in Canada right now," says John Boscariol, partner of the law firm McCarthy Tétrault in Toronto. "We've had a number of things happen just in the last few months."

On Aug. 15, Justice Charles Hackland of the Ontario Superior Court of Justice rendered a guilty plea against an individual for conspiring to pay bribes to government officials in India in violation of Canada's Corruption of Foreign Public Officials Act. The case marks the first time in the 14-year history of CFPOA that a foreign bribery case has ever been tried.

Since its passage in 1999, the CFPOA—Canada's version of the U.S. Foreign Corrupt Practices Act—has prohibited Canadian companies and individuals from bribing foreign officials. Three companies have been convicted under the CFPOA, but they all pleaded guilty.

"The case sends a message that Canadian authorities are not just concerned with going after companies, that individuals are being pursued as well," says Boscariol. "As an individual, you can't hide behind a company."

According to the charges, first filed in 2010, Nazir Karigar offered $450,000 in bribes to the Indian Minister of Civil Aviation and officials of Air India, which is owned and controlled by the Government of India, in an attempt to secure a multi-million dollar contract to supply a security system.

At the time, Karigar was serving as an advisor for Cryptometrics Canada, a subsidiary of tech security company Cryptometrics USA. Karigar argued that Canada had no jurisdiction over his activities because the events in question didn't occur within the territory of Canada, and because Cryptometrics was controlled by executives based in the United States.

Hackland disagreed, finding a "real and substantial connection" to Canada because Karigar is a Canadian and bribes benefited the Canadian security company, not its U.S. affiliate.

Even though this case concerns the willful misconduct of a rogue individual, Boscariol says the warning for companies is that they can be found in violation of the law where Canadian authorities can prove conspiracy to commit a bribe, without having to show a bribe was actually received.

Canada has also significantly expanded the grounds for criminal liability for companies and their directors, officers, and employees under recent amendments to the CFPOA.

The revised law, finalized in June, now includes a separate criminal "books and records" offense for misrepresenting or concealing the bribery of a foreign public official in their recordkeeping. And it increases the maximum jail sentence for individuals from 5 to 14 years.

The law also expands the scope of liability. Canadian companies and individuals who are involved in the bribery of foreign public officials are now subject to Canadian law regardless of where the bribery took place, and even if they have no connection with Canada other than their nationality.

Unlike the FCPA, which includes an exception for facilitation payments, Canada's anti-bribery law phases out the exception allowing facilitation payments, bringing it more in line with the U.K. Bribery Act, which also prohibits certain facilitation payments.

To address this discrepancy, many multinational compa-

nies have gone the route of adopting a uniform set of policies that meet the high watermark of the most stringent requirements. "More companies are just saying no to facilitation payments. Period," says Friedman.

New Laws in Place

While some countries are bulking up enforcement of their anti-bribery laws that have been on the books for years, others are adding new anti-bribery laws or tightening existing ones.

In August, for example, Brazil's President Dilma Rousseff signed into law the Clean Companies Act—Brazil's first anti-corruption law targeting companies. Prior to the law's enactment, only individuals could be prosecuted for corruption.

In some respects, Brazil's anti-corruption law goes even further than the FCPA—at least on paper—by prohibiting not just bribery, but also fraud in public procurement, bid rigging, and contracts with public bodies. Similar to the U.K. Bribery Act and Canada's CFPOA, Brazil's anti-corruption law also prohibits facilitation payments.

The new law, which will take effect on Jan. 24, 2014, also establishes strict civil and administrative (although not criminal) liability for the bribery acts of corporate directors, officers, employees, and other agents acting on a company's behalf. "Any U.S. company that does business in Brazil, even if it doesn't have a subsidiary in Brazil, may be subject to the law," says Felipe Berer, of counsel for law firm Akerman.

A company found guilty of corruption can face stiff penalties as well, including fines of up to 20 percent of its gross revenue from the previous year. Other penalties can include disgorgement of benefits obtained, suspension of the company's activities, or even dissolution of the entity.

The good news for companies is that Brazilian law includes a provision directing that sanctions may be reduced for companies with effective compliance programs in place and those that self-disclose violations of the law to authorities.

"Prior to these amendments, companies did not get credit for having state-of-the-art-compliance programs," says Carlos Ayres, a lawyer with Trench, Rossi & Watanabe in Sao Paolo. Nor did they receive any credit for self-disclosure and cooperation for matters relating to corruption. "So these are very welcome developments," he says.

Still, plenty of skepticism remains as to what extent Brazilian authorities will enforce the new law once it goes into effect next year. "Brazil is definitely known for having good laws on the books, but when it comes to enforcement, that's a completely different story," says Berer.

What's on the books right now is a three-page, broad-stroked law, says Berer. "They need to come up with the fine print." For example, the law does not make clear whether payments to political parties are covered, he says.

India now remains the only BRIC country that has yet to enact legislation prohibiting the bribery of foreign officials by companies operating within the country. China and Russia enacted such legislation in 2011.

Unlike the United States, neither Canada nor Brazil currently offer any guidance or detail on what they consider to be the elements of a robust anti-corruption compliance program. Therefore, legal experts advise companies to follow other guidelines, such as the FCPA Resource Guide, or those provided by the Organization for Economic Co-operation and Development.

With other countries stepping up enforcement of foreign bribery, U.S. companies should be careful not to put in place an overly U.S.-centric compliance program, Berer adds. For any country the company conducts business with, you have to make an invested effort to understand not just the country's unique culture, but also that of the company itself, he says. "That's more important than coming up with a complex compliance program that simply doesn't work." ■

TERRITORIAL JURISDICTION

Below is an excerpt from the Ontario Superior Court Ruling between *Her Majesty the Queen and Nazir Karigar.*

The accused argues that Canada lacks territorial jurisdiction to try this offense.

Bill S-14 has as one of its primary purposes to amend the CFPOA to establish "nationality jurisdiction" as a basis for Canadian Courts to exercise jurisdiction over persons accused of violating the CFPOA. In other words, jurisdiction over the bribery of a foreign public official based on the nationality of the offender i.e. his or her Canadian citizenship, is a new jurisdictional basis similar to the court's jurisdiction currently exercised on this basis over certain sexual offences against children and terrorism offences. However, these recent changes to the Act are not retroactive and do not apply to the present case.

Under the CFPOA applicable at the time of the trial of the present case, in order for this court to exercise jurisdiction over the offence, the Crown must prove that there was a "real and substantial link" between the offence and Canada, based on the principles set out by the Supreme Court of Canada in *Libman v. The Queen* [1985 2 S.C.R. 278. I reviewed this issue in an earlier application for prohibition in the present case, see 2012 ONSC 2730. I granted leave to the accused to raise the jurisdictional argument at trial at the close of the Crown's case. It was agreed that the court would deal with the argument as a substantive defence.

Source: Ontario Superior Court Ruling.

Corruption Risk Rising in China, Russia, Mexico

A focus on mitigating corruption has done little to curb BRIC nation fraud

By Jaclyn Jaeger

Despite an intense focus on mitigating corruption risks, the perils are only increasing for companies that do business in places like China, Russia, and Mexico.

Vigorous enforcement of the Foreign Corrupt Practices Act by the Justice Department and worsening corruption in several countries are making it increasingly difficult to get corruption risks under control for companies that are expanding globally. Those risks are upping the ante on the importance of conducting effective cross-border investigations.

Despite cultural differences or the lack of transparency in some countries, the Department of Justice has made clear that no country is immune from FCPA enforcement. As Assistant Attorney General Lanny Breuer recently stated during a conference on the FCPA, "Combating corruption around the world is, and will remain, a priority of the United States."

At the same time, as more U.S. companies are increasing their global operations into BRIC nations—Brazil, Russia, India, China—and Mexico where the FCPA often creates the greatest compliance headaches, "they will necessarily have to align their anti-corruption compliance efforts with the global enforcement environment, or risk paying a very high price for failing to do so," says Kelly Currie, a partner with law firm Crowell & Moring.

That means multinational companies doing business in BRIC countries and Mexico must tailor their policies and practices to each jurisdiction in order to avoid the unique bribery risks that innately arise while conducting business in these countries.

If you look at FCPA enforcement over the last decade, the industries that are most vulnerable to corruption tend to be those with state-owned or state-operated entities, including energy, oil and gas, mining, telecommunications, and healthcare companies. "Foreign bribery is certainly not limited to those industries, but those are the areas in the past that have shown a high level of bribery," says Paul Pelletier, a member of the law firm Mintz Levin and a former federal prosecutor of the Justice Department.

Consider the $236 million settlement that the Justice Department and Securities and Exchange Commission reached with global freight forwarding company Panalpina World Transport and six of its customers—GlobalSantaFe, Noble Corp., Pride International, Shell, Tidewater, and Transocean—for paying thousands of bribes from 2002 through 2007 to foreign officials for customs clearance in several countries, including Brazil and Russia.

There are some signs that corruption is declining in some BRIC countries. Brazil and India, for example, have moved up—albeit only slightly—on Transparency International's Corruption Perception Index, since last year's rankings. With a rank of 73 in 2012, Brazil moved up four spots to 69 this year. In comparison, India moved up one spot from 95 to 94. Given that Transparency International ranked eight more countries than last year, actual progress in Brazil and India remains difficult to determine.

"The good news is that the more that western companies enter into these markets, the more that these markets become more open, more transparent and, therefore, more compliant with anti-corruption laws," says Paul Berger, a partner in the law firm Debevoise & Plimpton. In some BRIC countries, for example, U.S. companies are finding that state-owned entities and government officials are operating in a much more transparent way than just a decade ago, he adds.

But with progress comes some setbacks. China is the only country of the BRICs that fell in the Transparency International rankings from the 75 spot in 2011, down to the 80 spot in 2012. Mexico's rankings on the Corruption Index also declined from the 100 spot in 2011 to the 105 spot in 2012. And while Russia's rank improved to 133 out of 174 countries in the 2012 Corruption Index, up from the 143 out of 182 countries ranked last year, it remains the most corrupt of the BRIC countries to do business with.

In Transparency International's Global Corruption Barometer, the only worldwide public opinion survey on corruption, which interviewed more than 100,000 respondents in 100 countries, 53 percent said they believe corruption has increased in Russia, whereas 39 percent said it has stayed the same. Only eight percent said that corruption has decreased. When asked how they would assess the government's fight against corruption, the majority (52 percent) described it as "ineffective."

Each of these countries also presents its own unique country-specific bribery risks, due to their diverse cultures, government structures, and business operations. As companies move into different markets and their business models change, says Currie, "your assessment of corruption risk has to continually evolve with your changing business model.

Political scandals in Brazil and India, for example, represent an emerging issue that has brought potential FCPA violations to light over the last couple of years, says Currie,

when they have involved allegations of corruption—such as kickback schemes tied to the awarding of contracts—linked to U.S. companies. "The U.S. authorities open an investigation focused on the company making the alleged corrupt payments, while the local attention is on the politicians and government officials," says Currie.

Such high levels of corruption among political parties also are reflected in Transparency International's Global Corruption Barometer, in which respondents in Brazil and India ranked political parties as the most corrupt out of eleven organizations; parliament members and police also received high corrupt rankings in both countries.

Matthias Kleinhempel, director of the Center for Governance and Transparency at IAE Business School of Austral University in Buenos Aires, points out that Brazil has recently made great strides in its anti-corruption efforts. "If you look at the progress of improvement," he says, "you can see that the government has made very clear and consistent efforts to prosecute corrupt officials."

In November, for example, the Supreme Court of Brazil convicted Jose Dirceu, the chief of staff of former President Luiz Inácio Lula da Silva, over charges that he laundered and doled out millions of dollars in public and private money to secure votes for legislation in the National Congress from 2003 to 2005. He was sentenced to nearly 11 years in prison. Twenty-two other individuals, including politicians, aides, and bankers also were convicted on various charges.

China Expectations

In China, on the other hand, the cultural expectation of treating government officials with gifts, travel, and entertainment as a way of showing respect highlights the need for strong controls and policies around such practices. Bribery can come in the form of theater tickets, trips, loans, expensive meals, education, political or charitable donations, club memberships, and more.

Global beauty company Avon Products learned this lesson the hard way, when the company commenced an internal investigation in June 2008 after a whistleblower alerted executives that certain travel, entertainment, and other expenses may have been improperly incurred in connection with the company's China operations.

The Avon case is also a lesson in how expensive conducting a global FCPA investigation can be. Since 2009, Avon has spent a whopping $247 million on professional and related fees associated with the global FCPA investigation and compliance reviews. A breakdown of those costs shows the company spent $93.3 million in 2011, $95 million in 2010, and $59 million in 2009.

Another risk that is unique to doing business in countries like China and Mexico is the prevalent use of cash. "China, for example, is still a very cash-oriented society," says Berger. "It's not unusual for businesses to want to be paid in cash."

Doing business in this manner, however, greatly enhances the risk of bribery payments and, thus, the chance of an FCPA investigation. Just consider the case of Control Components, which pleaded guilty in July 2009 after paying millions in cash, vacations, and other gifts from 2003 to 2007 to officials and employees of foreign state-owned companies in China and various other places in order to win business.

U.S. companies will often enlist the help of third-party agents, consultants, or intermediaries who are familiar with the inner workings of these countries and can help cut through the red tape. The compliance challenge there is making sure that the third parties or consultants who live locally in that country and work on the company's behalf are "not accepting of local customs or practices that run afoul of the FCPA," says Pelletier.

This means vetting third-party intermediaries, practicing continuous due diligence while engaging in business with them, maintaining accurate books and records, and conducting internal investigations into potential FCPA violations.

With global anti-corruption enforcement expected to rise and U.S. prosecutors cooperating with foreign law enforcement on FCPA cases more closely than ever before, the free-flow of investigative information between and among regulators and law enforcement agencies in these countries, Currie says, is also going "to feed the quantity and quality of the investigations that we see." ■

CORRUPTION IN BRIC NATIONS

Respondents to the Global Corruption Barometer, 2010/11, were asked: "In the past three years, how has the level of corruption in this country changed?" Percentages based on their responses are below.

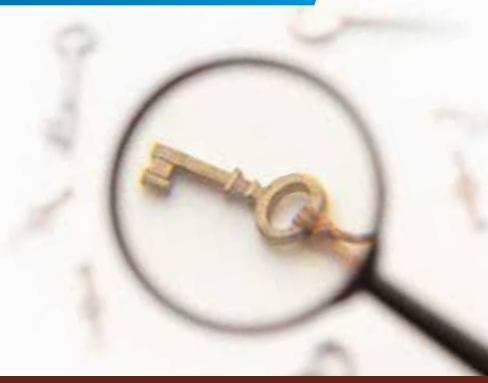
Country	Decreased %	Same %	Increased %
Brazil	9	27	64
Russia	8	39	53
India	10	16	74
China	25	29	46

Source: Global Corruption Barometer (2010, 2011).

KPMG
cutting through complexity

ForensicFocus

Hiding in plain sight: The anatomy of a bribe



TODAY'S REALITY

- Operating in foreign countries carries the risk of bribery and corruption.
- Bribes can lurk anywhere that there is contact with foreign officials.
- Bribes are most often camouflaged as legitimate payments.
- There are many types of bribes, and they can live in both the supply and sales channels.

Enforcement of anti-bribery and corruption laws around the world is at an all-time high. Regulators are attacking corruption by wielding older weapons, such as the 1977 U.S. Foreign Corrupt Practices Act (FCPA), and by using new ammunition like the 2010 U.K. Bribery Act.

If your company does business in any foreign country, there's a risk that bribes could be hiding in plain sight. To know what they look like and where to find them, you first need to understand the anatomy of a bribe.

What Is a Bribe?

The dictionary defines a "bribe" as "money or favor given or promised in order to influence the judgment or conduct of a person in a position of trust." Yet its meaning under most global anti-bribery and corruption laws is much more nuanced.

Example: The FCPA prohibits paying, offering, or promising to pay "anything of value" to a foreign government official or instrumentality in order to obtain or retain business. There's no minimum monetary threshold. Whatever is paid or promised can have an intangible value, and it can be received only beneficially by the recipient.

A bribe also must be intended to corruptly induce the recipient to misuse an official position. The U.K. Bribery Act defines a bribe as being a "financial or other advantage" and does not require corrupt intent. The Anti-Bribery Convention of the Organization for Economic Cooperation and Development, which has been signed by 39 countries, defines a bribe as any "undue pecuniary or other advantage" that was made intentionally.

What Are the Exceptions?

Under the FCPA, payments that otherwise would be bribes aren't prohibited if they are made to facilitate or expedite routine governmental actions, such as issuing permits or licenses. A payment or promise that would constitute a bribe under the FCPA also isn't prohibited if it is legal under the written laws of the applicable foreign country.

Most anti-bribery and corruption laws permit payments to foreign government officials for bona fide hospitality, promotion, product demonstration, and other business expenditures that are proportionate and reasonable.

On the Trail of Bribes

Periodic proactive risk assessments should be conducted to pinpoint areas where the business may be most vulnerable. Armed with this risk profile, internal controls can be implemented strategically and testing can be aimed precisely. Bribes most often are camouflaged as legitimate payments. They may take cover in both the supply channel and the sales channel, and they may be propagated by third parties.

Look for foreign government contacts with your organization. These may be direct contacts, such as interacting with government agencies that regulate business licenses, taxes (VAT), customs, import/export, real estate, transportation/shipping, utilities, and product certifications or approvals. Foreign government contacts also occur indirectly through third-party intermediaries. Closely monitor those that carry the greatest risk: brokers, agents, shippers, custom logistics, resellers, and distributors delivering services that interact with foreign officials.

© 2013 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Sufficient background research needs to be conducted on vendors, suppliers, and agents to ensure that you are dealing only with reputable third parties. You must determine if any third parties are owned or controlled by current or former foreign officials, or by people closely affiliated with these officials. Sophisticated corporate intelligence tools can provide various levels of reputational due diligence.

Where Do Bribes Hide?

Look for insufficient or nonexistent descriptions of the transaction, lack of proper support, and specious business rationale for the transaction. Conducting trend analyses and data analytics on these accounts can expose anomalies that might point to a hiding place. Taking a risk-based judgmental sample of transactions for testing can be based on certain risk factors (e.g., the kind of counterparties, the geographical location of counterparties, the stated purpose of the transaction, and the likelihood of government touch points).

Common Hideouts

- Expense reimbursements for excessive travel and entertainment
- Petty cash and advances to employees
- Accounts payable
- Expense and disbursement logs
- Check and wire registers
- Inventory
- Cost of goods sold
- Sales and marketing expenses
- Rebates and discounts

Many bribes are relatively small in amount. It may be necessary to take samples of transactions and review supporting documentation to assess the legitimacy of a payment.

With travel and entertainment expenses, look for original receipt documentation; the names of individuals involved and the purpose of the event; proper approvals and timely submissions; reasonable exchange rates; and mathematical accuracy of the expense report.

Each document transmitted to or from your organization should be examined for a bribe's footprint. Bribes may hide in contracts and agreements, financing arrangements, invoices, purchase orders, bills of lading and shipping documents, bank statements, and written communications. Special attention should be paid to supplemental, modified, or last-issued invoices and purchase orders because many times a bribe is solicited after the initial business dealings. Sales contracts should be reviewed to assess the reasonableness of margins, commissions, and costs, as well as for vague terms, advance fees, large termination fees, or frequent undocumented change orders.

The most common types of disguises are special payments or fees; above-market commissions; business introduction fees; rebates or discounts; promotion and marketing expenses; inspection fees; political or charitable contributions; or unusual selling or distribution charges. More creative covers for bribes can be manipulations of currency exchange conversions; payments in other currencies; overstated product quantities or weights; overly complex financing terms; or unnecessary insurance/indemnity charges.

Simplifying the supply and sales channels can help. Many of the hiding places can be removed by eliminating third parties that aren't essential for business operation, by reducing complex procurement and distribution processes, and by creating uniform external documentation.

Identifying Bribes That Leave No Trace on the Books and Records

Preferential treatment or manipulation in the bidding or RFP process to select suppliers, vendors, or third-party agents can also be a breeding ground for bribes that rarely leave a trail.

Additionally, bribes may take the form of:

- Gifts
- Use of materials, equipment, facilities, or services
- Transportation and hospitality
- Offers of employment
- Scholarships and educational allowances

Another form of bribery is awarding work to a third party that's affiliated with a current or former foreign official or their family. This is especially true if the third party isn't qualified, can't deliver the service, or doesn't submit the lowest bid or quote. These types of bribes are extremely difficult to detect because they often don't leave a footprint anywhere in your organization. In many cases, the only way to detect one of these bribes is for someone to spot it and report it to the appropriate person.

What Can I Do Now?

Armed with understanding of what bribes are and where to look for them, the most effective way to ferret out bribes then becomes implementation of a comprehensive anti-bribery and corruption compliance program. But one size does not fit all. A compliance program must be tailored to accommodate your risk profile and resources.

By taking a proactive approach to preventing bribery, you can dramatically reduce the occurrence of bribery even in the most corrupt locations. Because bribes can live in so many different habitats, a comprehensive compliance program is like a net that can snare bribes wherever they hide...even in plain sight.

Author

Scott Hilsen
404-222-3015
shilsen@kpmg.com

kpmg.com

Contact us

North East	South East	Mid-West	Mid-Atlantic	South West	West
Marc Miller	**Phillip Ostwalt**	**Rocco deGrasse**	**Pamela Parizek**	**Michael Schwartz**	**Guido van Drunen**
212-872-6916	404-222-3327	312-665-1296	202-533-5362	713-319-2258	206-913-4208
marcmiller@kpmg.com	postwalt@kpmg.com	rdegrasse@kpmg.com	pparizek@kpmg.com	mschwartz@kpmg.com	gvandrunen@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2013 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International. NDPPS 149204

Managing the Exchange of Data Across Borders

By Jose Tabuena
Compliance Week Columnist

Cross-border transfer of information is an increasingly crucial and difficult component of conducting business around the globe, especially when it comes to cross-border investigations.

The challenges of data exchange for international companies are considerable as the requirements and repercussions are not uniform across jurisdictions. What is permissible in the United States may be forbidden in Europe or elsewhere. Internal auditors and compliance professionals at multinationals need to be cognizant of the rules regarding the transfer of data in the jurisdictions where they operate to ensure that actions taken in one geography of the business do not result in infractions in others.

Jose Tabuena
Columnist

One of the biggest risks is the potential of cyber-security breach. This concern is emerging as technology becomes more pervasive, Big Data emerges, and companies extend their reach internationally. The Internet doesn't recognize borders—as data is moved from the data center to the cloud and across borders, security breaches become a more tangible risk.

Numerous countries and the European Union have implemented privacy laws that typically forbid cross-border transfers unless certain conditions are met. There is considerable divergence, however, in definitions and how certain types of data are to be secured, which can create significant difficulties in transferring it. The Ponemon Institute in a study of privacy and data protection compliance for multinational organizations, for example, found that the varying data definitions result in higher compliance costs. This is not surprising to those who have to manage the regulatory complexity while trying to minimize disruption to business processes.

What Is Personal Data?

Most countries have data protection laws that govern how personal information relating to individuals may be processed. Personal data, also referred to as "personally identifiable information" (PII), is a core concept in privacy regulation as it defines the scopes and boundaries of privacy statutes and regulations around the world. Lawyers refer to PII as a *jurisdictional trigger* as in its absence there is no privacy right or harm to protect. Thus, privacy regulation focuses on the collection, storage, use, and disclosure of PII while leaving non-PII largely unprotected.

In the United States alone the lack of a uniform definition is a substantial burden, as it is a trigger for *breach notification requirements* in 48 jurisdictions (46 states plus D.C. and Puerto Rico). The PII definition varies so much within the United States that compliance professionals need to reference complex charts with links to statutes in order to monitor its meaning in a given state.

Currently, companies can move data between the EU countries and the United States under a formal "safe harbor" treaty between the two jurisdictions if the United States' party gets certification confirming its data procedures comply with principles set out in EU data law. The lack of clarity and harmony under the EU Data Protection Directive, however, gives rise to uncertainties relating to the maintenance and the location of PII, such as the use of cloud computing. Companies can still move data from Europe to other jurisdictions that the European Union has assessed as providing "adequate protection" of data, but there are not many countries that are so qualified. Moreover, with proposed regulation intended to update the framework for managing PII, the European Union has raised the possibility of scrapping this safe-harbor provision.

To compound the compliance challenges, the narrow focus by privacy regimes on data location made sense when data could be transported between countries only by physically carrying storage media across borders. With the inception of the Internet, the cloud, and the ease of electronic transfer and remote access to data, the concept of location is increasingly irrelevant to data protection.

A common misconception is that merely viewing data remotely is not subject to transfer restrictions. But in Europe it is accepted without question that remote access to PII is equivalent to the transfer itself of the data—information security experts recognize that to be able view the data, it has to be actually transmitting from the position it is stored to the location it is being seen.

There's no real regulatory guidance or case law specifically on this point, but when you consider that the purpose of the data export restriction is to prevent leakage of PII, then remote access presents precisely the same risk as a traditional transfer. Someone remotely accessing data that is hosted in another country could, after all, easy print, duplicate, or even write down and improperly disclose personal information.

How to Manage the Transfer Process

Given the regulatory uncertainty and the current disparity amongst privacy regimes and definitions of PII—particularly between the United States and European Union—how can a global company develop an efficient and compliant data transfer process? An organization with a robust privacy program is likely to have conducted a security

risk assessment with analysis of its compliance vulnerabilities. Presumably the company is collecting the data they're generating and tracking so they know where they have it. At minimum the organization should have:

» Performed a comprehensive data discovery process to find all of its PII and other critical data;

» Determined the lines of business affected by privacy laws and regulations such as Health Insurance Portability and Accountability Act (HIPAA) in the United States and the EU Data Protection Directive; and

» Mapped the movement of customer PII and other sensitive and confidential information within the organization, including data flows to and from third parties.

> Internal auditors and compliance professionals at multinationals need to be cognizant of the rules regarding the transfer of data in the jurisdictions where they operate to ensure that actions taken in one geography of the business do not result in infractions in others.

The internal audit and compliance functions are well-situated to support effective company information practices that can facilitate the secure transfer of sensitive data across borders. Audit and compliance can also aid in creating processes that considers the management of PII over a range of security objectives, rather than by using a simple dichotomy.

Keep in mind that the main difficulty is advancing a consistent approach that navigates the disparate definitions of PII. With continued advances in information technology, the task of defining PII is likely to undergo transformation. There have been recent experiences displaying the potential of Big Data and the power of correlation. What is not considered PII today could easily become PII in the future as the ability to link pieces of data to specific individuals becomes more prevalent. It is the typical experience of legal concepts lagging behind changing technology.

Multinationals need to be aware that the European Union has the strictest privacy regime. Tailoring a data approach that incorporates EU principles may ultimately afford the most flexibility. Any approach should consider the applicability of what is referred to by privacy practitioners as fair information practices built around different levels of risk to individuals.

Compliance and privacy programs will need to be alert in this rapidly evolving area. Computer science has shown that the very concept of PII is far from straightforward. The ability to "identify" depends more on context including technology as well as social and corporate practices. The varying definitions of PII threaten the utility of mechanisms for allowing the data transfers. The current safe harbors that are typically bilateral may be on the way out.

More organizations that operate in Europe are now examining the use of Binding Corporate Rules (BCRs) as they approach a more global harmonized solution being sought by the European Union. BCRs permit data transfers between entities globally, whereas the EU-U.S. Safe Harbor is limited to data transferred between those two regions. However, BCRs are not for the faint of heart and require a commitment in terms of resource, time, and cost.

BCRs are an affirmative statement of taking data protection seriously, which will require extensive project management by the compliance program to develop and implement. Fortunately, BCR standards sync well with other data protection initiatives including many state laws and the HIPAA. The very specific things that U.S. law requires with various types of data also fit nicely with the EU concept of data privacy and, further, into what BCRs require to do to protect data—such as consulting agreements, audits, risk management, breach reporting, and other measures.

Many commentators foresee more unified and revised privacy frameworks that take into account new technologies that impact current definitions of PII. Awareness is growing that the focus of standards on data location should not obscure the underlying purpose of the data export restriction—which is ensuring data protection. The specific objective for restricting data transfer of PII was, and remains, to protect personal data against access by unauthorized persons. Where technology can be applied—data strongly encrypted and the decryption keys securely managed, for example—the data's location should be immaterial. Conversely, keeping data within a particular geography does not guarantee better protection if it is not secure. ■

Jose Tabuena is compliance and regulatory counsel with Orion Health, a global provider of clinical workflow and health data integration technologies and solutions. He writes a column every other month on internal auditing and compliance program challenges offering a unique perspective on internal auditing issues bringing Big Four firm experience and having held a variety of audit-related roles, including compliance auditor, risk manager, corporate counsel, and chief compliance officer. Mr. Tabuena is certified as a fraud examiner, in healthcare compliance, and is an OCEG Fellow.

Tabuena can be reached at jtabuena@complianceweek.com.

Cultural Norms in China That Snag Compliance

By Jaclyn Jaeger

China is emerging not just as a massive and powerful economy, but for the companies that do business there, as a huge compliance risk. It's also a particularly thorny place to conduct internal investigations.

China's anti-bribery enforcement, in particular, has grown significantly stronger over the last year, forcing U.S. companies that operate there to consider not just compliance with the U.S. Foreign Corrupt Practices Act, but local Chinese anti-bribery laws. "Businesses seem to be recognizing, rightly so, a culture of greater enforcement by China on anti-bribery and corruption issues," says Randy Stephens, vice president of Advisory Services at Navex Global.


Stephens

As a result, U.S. companies have no choice but to understand and respect the cultural differences, and obstacles, that come along with doing business in China in order to reduce their corruption and bribery risks. And companies must tread carefully when conducting investigations to avoid getting tripped up by these cultural norms.

1. Tight-knit personal networks

The old expression, "it's not what you know, it's who you know," is far from cliché in Chinese culture. Familism has great influence on business decisions, "particularly since many of China's companies are family based," says Violet Ho, senior managing director in the Greater China practice at risk consultancy firm Kroll.

"Foreign management may find it hard to penetrate this family circle of trust and secure loyalty, making it challenging to enforce their decisions," explains Ho. "Familism may cause compliance concerns and make it all too easy for management at the China branch to circumvent anti-corruption measures put in place by the head office."

Most Chinese companies also possess tightly-knit networks of informal interpersonal ties and relationships, including those with the Chinese government, known in Chinese culture as "guanxi," which is a "central idea in Chinese society," Ho adds. "Guanxi for some companies may mean they are more likely than their competitors to be approved for loans, or they may receive relevant licenses sooner."

"There is still very much an overriding culture of 'us' and 'them' in China, and the 'them' doesn't necessarily have to be non-Chinese," says Louise Kern, managing director of consulting firm GloBIS, which helps companies entering the China market.

"Chinese companies can still be very focused on just doing business within their own known networks," Kern adds. "If a company is not within their circle of acquaintance, anything is fair game."

Such relationships make it especially challenging for foreign companies to do business in China if they're not part of these networks. "Any personal relationship you can build is hugely important for your business relationship with a Chinese company," says Kern.

Because many relationships in Chinese culture are built on mutual trust and respect, any sort of conflict can pose a threat. A U.S. company coming into the country to investigate potential violations of the FCPA, for example, is never an easy process.

"Americans want to put an issue on the table, have a thoughtful discussion about it, provide facts of both sides, and hope to reach a common understanding and way forth," explains Brian Wilson, a managing director with KPMG's advisory services. "In China, it's very difficult to put issues on the table culturally, because you could be causing the counterparty to lose face."

This can be particularly frustrating for a U.S. company, "especially when you're trying to move fast and trying to get information out of an operating company on exactly what happened, and when," says Wilson. A conflict can be resolved a lot faster by having a local team who understands these cultural differences, he advises.

2. Pro-employee rights

Employee rights are extremely favorable in Chinese culture, making it incredibly difficult to terminate an employee who has engaged in fraud or corruption. "You have to really prove a pattern of misconduct over time," says Wilson.

Even if the employee has engaged in one or two acts of egregious wrongdoing, "that won't be enough to prove intentional misconduct," Wilson adds. If a decision is made to terminate an employee, you need to have a robust story and be prepared to defend that story to China's labor bureau if the employee files a termination lawsuit, he says.

3. Widespread collusion

Conflicts of interest, fraud and corruption, embezzlement, and kickbacks are all common practice in China, and "all occur outside the four walls of Chinese companies," says John MacPherson, director of the Crisis and Security consulting practice Control Risks for the Greater China region. "Generally, U.S. companies don't have that depth of understanding to know how to respond to that sort of external environment."

It's not atypical in China for there to be an "elaborate tribe of sales people who are very loyal to each other, and not loyal to the multinational company that they work for," says MacPherson. "They actively collude to set up their own

> "In China, it's very difficult to put issues on the table culturally, because you could be causing the counterparty to lose face."
>
> Brian Wilson, Managing Director, KPMG

distribution network to achieve personal gain."

Bribes and money laundering paid through marketing agents or travel companies, for example, often are "completely off the books," and can be missed by auditing and compliance programs, MacPherson adds. "It's forcing a lot of companies to have to reevaluate their compliance and audit programs."

Wilson says that means having to do more face-to-face interviews with third parties, as well as potential joint venture partners, to get a better understanding of where revenues are coming from, and going to.

4. Restricted access to corporate information

The ability of U.S. companies to obtain information about domestic Chinese companies from government corporate registration agencies is often very difficult, due to a lack of publicly available information. "Sometimes it depends on what level of access regulators want to give you," says Wilson.

China's State Administration for Industry and Commerce, for example, maintains the official corporate files and corporate information on companies incorporated in China. Such information typically includes a company's name, date of establishment, business address, the names of its shareholders, among other details. "That information today is generally not available in most of the jurisdictions in China," says Wilson.

Wilson

U.S. companies are finding it "increasingly challenging" to establish a straight line of sight on their third-party business partners, which is forcing them to come up with alternative solutions to their due diligence practices, says Wilson. If a U.S. company wants to do a joint venture with a Chinese company, for example, it may be more effective to obtain information directly from the company itself, whereas in the past such information would have been obtained by a third party, or the proper government agency, he says.

5. Conflicts with compliance directives

For foreign companies operating in China, a common practice is to import their anti-corruption policies and procedures from their developed home markets, and then expect that those standards will be followed without really understanding or appreciating the external operating environment.

"They assume that the Chinese workforce will be able to exercise the same level of judgment that we expect of employees outside of China," MacPherson says. "That's consistently proven to not be the case."

Employees in the local market are stuck balancing between meeting the cultural expectations of the company versus that of the [country's] culture, says Wilson. "There ends up being this disconnect of actual compliance in a local market versus the program's true design," he says.

Most well-established anti-corruption programs, for example, carry out due diligence on third-party partners—such as distributors, deal-brokers or suppliers—where the potential for fraud is high, Ho says. In China, however, "it is necessary to widen the scope of due diligence on third-party relationships to also include advertising agencies, travel agents, or event organizers, which would typically be considered low-risk in most developed markets," she says.

Wilson recommends creating policies and procedures that are conducive to the local employees in that country. That means using "practical examples that are communicated in the local language to local sales force," he says.

"You have to educate your workforce and third parties on the nuances," adds Stephens. "What is acceptable and legal in that country may be something that is contrary to the code of conduct of a U.S.-based company."

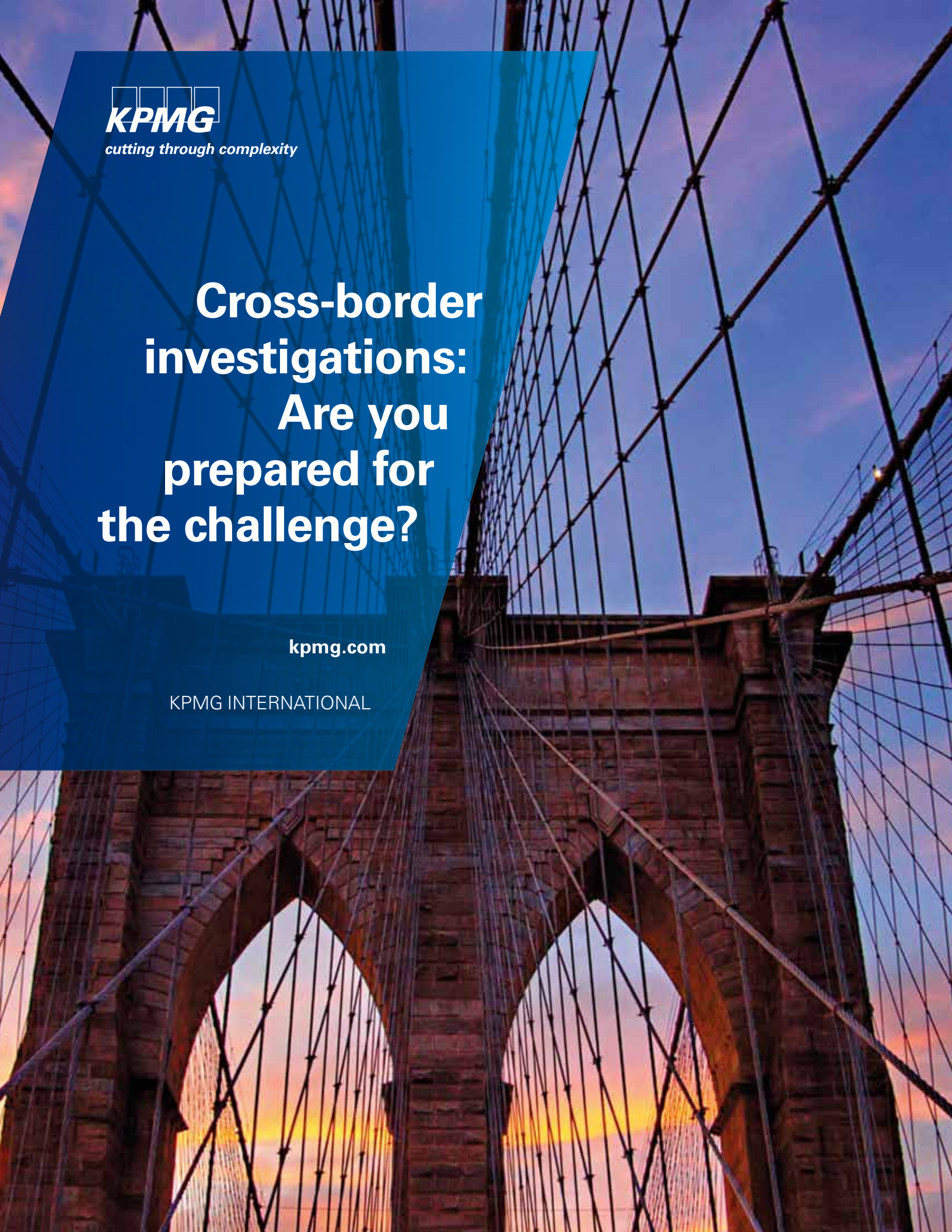
Much of the premise for effectively doing business in China lies in knowing how to adapt to their culture, experts say, rather than relying on them adapting to you. ■

DOING BUSINESS IN CHINA

Foreign companies operating in China can take several steps to mitigate bribery and corruption, while doing business in the country. Violet Ho, senior managing director in the Greater China practice at risk consultancy firm Kroll, offers the following advice:

1. Look carefully at any potential local partner's track record on compliance and ethical conduct. When hiring a local manager, do not assume that strong local expertise negates the need for thorough due diligence.
2. When putting in place anti-corruption measures locally, these will only be of value if managed by a local team put in place by the head office.
3. It's important for someone from U.S. headquarters to visit the local China site regularly rather than relying on a quarterly report from your subsidiary. Sometimes these visits should be done with little advance warning.
4. Build and maintain your own relationships with government regulators and don't just rely on local senior management

—Violet Ho



KPMG

cutting through complexity

Cross-border investigations: Are you prepared for the challenge?

kpmg.com

KPMG INTERNATIONAL

01 Introduction

Conducting cross-border investigations is no simple endeavor. Add the complexities of legal and cultural differences, and you have arguably one of the biggest challenges facing global corporations today. There are obstacles at every step of a cross-border investigation, including initially receiving a claim or allegation; complying with foreign data privacy laws; using the appropriate staff and resources; respecting diverse employee rights; and remediating across borders. Understanding where the pitfalls are along the way and how to navigate them can help you avoid critical missteps.

The goal of this paper is to give you meaningful guidance by discussing ways to effectively meet these challenges through the experiences of KPMG investigations professionals working around the world. In addition, we asked sixty worldwide executives who are responsible for managing their organizations' cross-border investigations to tell us about the challenges and obstacles they regularly face. Ninety-five percent of these executives said that they expect their needs for cross-border investigations to increase or at least to stay the same over the next year. We are pleased to share many of their other observations with you as well.

I sincerely hope you find this paper an interesting and useful resource.

Petrus Marais
Global Forensic Chair
KPMG Forensic

Phil Ostwalt
Global Investigations Network Leader
KPMG in the US

© 2013 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

02 Triggering a cross-border investigation

Cross-border investigations can be triggered from a multitude of foreign countries, in a variety of languages, through different reporting channels, and at anytime around the clock. It is critical, therefore, when designing intake procedures to receive and process allegations to use a global mindset and consider cultural differences. "How a company initially receives and reacts to an allegation of fraud can be a defining point in a cross-border investigation," says Alex Plavsic, KPMG in the UK. Unique challenges exist when an investigation originates in a foreign jurisdiction. "If proper translations of an allegation are not made, for example, or if certain people are not notified in a timely manner about a claim, the investigation will be fraught with problems from the beginning," Plavsic explains. In today's hyper-connected world it is not only possible but imperative to have well controlled and efficient processes that allow business to respond to allegations with the appropriate level of care, insight, and promptness. The reality is many companies may receive complaints, especially those from outside their home countries, and do not have a plan to deal with them. Understanding the ways in which a cross-border investigation can arise and how to respond can ensure that it starts out on the right track.

The most common trigger of a cross-border investigation is a lead or an allegation made by an employee of the company. Seventy seven percent of the respondents in KPMG's survey indicated that internal reporting triggered their most recent cross-border investigation. Almost half of these internal leads came through whistleblower and hotline programs, a notable figure given that cultures can differ widely regarding the acceptability of reporting the conduct of others. "In some cultures, a senior person can be committing a very blatant fraud, but no one under that person would ever think of telling someone about it. One does not go against superiors in some places," says Mark Leishman, KPMG in Australia.

In addition to cultural differences, the laws and regulations governing hotlines vary greatly from country to country. Data privacy laws in Europe, for instance, may restrict the use of whistleblower hotlines or even prohibit them from accepting anonymous calls. Some European Union countries require government approval or at least notification before establishing a hotline, while other countries compel companies to consult with employees and sometimes to get their consent before launching a hotline. Knowing the local culture and regulations about the triggers of cross-border investigations can help companies customize reporting channels to best fit the ways in which foreign employees might report allegations.

Case Study

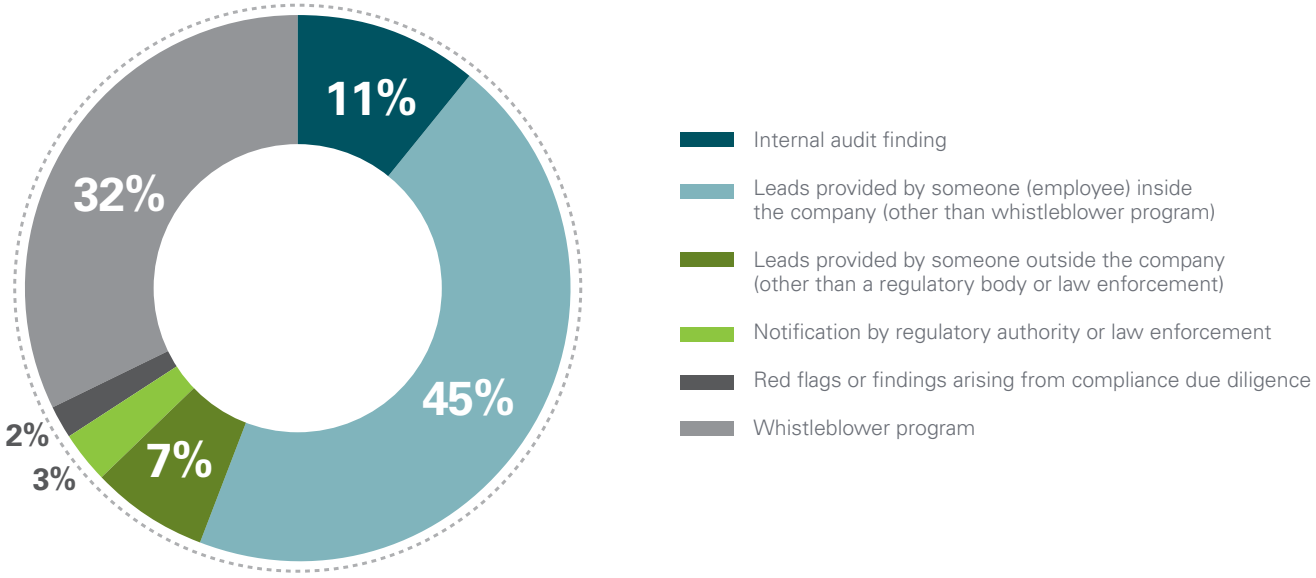
When a US-based consumer products company received hotline reports in foreign languages, the reports were immediately delegated to the country manager in the local jurisdiction to conduct an investigation. However, the company did not have a language-skilled person reviewing the reports before they were delegated. As a result, a report alleging potential corruption involving a customs broker in Germany was sent to be investigated by the country manager who was the actual person accused of the alleged wrongdoing. A well-designed intake process would have prevented this mistake.

© 2013 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

When a lead or an allegation is received in a foreign language, it is critical to get an accurate translation because even a minor misinterpretation can lead to a significant misstep. Online translation websites are no substitute for a language-skilled person who knows your business and is trained to review allegations. For instance, although Mandarin is the national language across China, the proper use of characters, sentence structure, and formation of clear thoughts varies dramatically from person to person and is heavily influenced by the upbringing of the individual, which an automated website cannot detect. It comes as no surprise that language differences present challenges in cross-border investigations for more than a third of the respondents to KPMG's survey. Companies, therefore, need to have hotlines that are staffed with appropriate language-skilled operators and to ensure that translations are accurate. "Before acting on a translation of a report, consult with someone in the country who knows not only the language, but also local sayings, common euphemisms, and double meanings of certain words," advises Shelley Hayes, KPMG in Mexico.

There are other important differences between the intake of allegations in domestic and cross-border investigations. Some countries require notification to an employee who is the subject of an allegation as well as notification to employee representatives or work councils, especially if the employee's data will be reviewed. Confidentiality laws also may restrict to whom a company can disclose an allegation, even internally. Because the labor laws and data privacy laws in many countries can seem counterintuitive to common practices, it is critical to understand them at the initial intake stage of an investigation.

Which of the following has been the primary trigger of most of your company's recent cross-border investigations?



Source: *Cross-border investigations: Are you prepared for the challenge?,* KPMG International 2013.

© 2013 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

03 Triage and protocol for cross-border investigations

Around the globe, employees have become empowered to raise concerns through a variety of reporting channels. For this reason, a company needs to be prepared to act quickly, efficiently, and effectively when responding to allegations. "Given the velocity with which compliance happens, management can never be prepared enough when it comes to its investigation protocols and procedures," noted Timothy Hedley, KPMG in the US. Many companies, however, are underprepared to meet this challenge. More than half of those who responded to KPMG's survey said that their companies have limited or no protocols for cross-border investigations.

A company's intake processes and its investigation protocols can be seen as two sides of the same coin. "The imperative of encouraging employees around the world to come forward with legal, compliance, and ethics questions cannot be realized unless a company also has appropriate investigative protocols and effective responses when issues are raised," says Richard Girgenti, KPMG in the US. Reporting mechanisms will quickly lose credibility among international employees if their concerns are disregarded or are handled poorly. For this reason, compliance officers, in-house counsel, human resources professionals, and other members of management who work for multinational companies need to be prepared to respond to allegations in a planned and consistent manner.

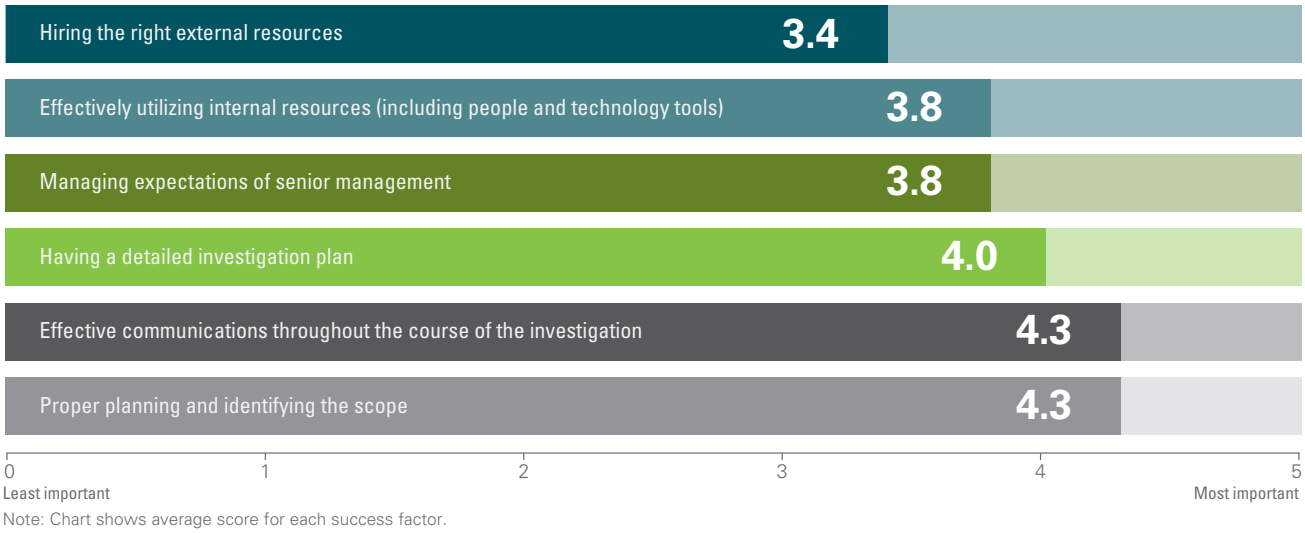
This means that a company should proactively develop case management and investigative procedures that align with the company's values, standards, and principles and take into account region-specific or country-specific requirements, customs, and practices. Oftentimes, one size does not fit all, and procedures will need to be customized to meet the requirements of a particular jurisdiction. Creating regional case management templates that highlight key procedural distinctions provides a good starting point. "As with most compliance initiatives, the development of case management and investigative policies and procedures should be a collaborative exercise between compliance leaders at headquarters and their colleagues around the world," says Maurice L. Crescenzi, Jr., KPMG in the US.

While many of the essential procedures of an effective domestic investigation and a cross-border investigation are the same, there are certain fundamental differences that case managers and investigators need to bear in mind. These differences include: the timeframe within which an investigation must occur; data privacy and the transfer of information; notifications to employees or their representatives; notifications to governmental agencies or law enforcement; and deadlines for reporting disciplinary measures taken by the company. Such fundamental differences can vary widely, depending on the jurisdiction where the investigation takes place.

"There should be a fundamental difference between the mindset of a case manager or investigator conducting an investigation on foreign soil," says Phil Ostwalt, KPMG in the US. "In fact, there are many differences. For instance, case managers need to remember that employment law may differ significantly from country to country." Additionally, case managers and investigators need to be adaptable to the investigative procedures and strategies that can lead to success at the local level. Given these jurisdictional and cultural differences, certain tactics considered effective in a particular country may prove counterproductive in certain foreign settings.

© 2013 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

How important are the following to the execution of a successful cross-border investigation?



Note: Chart shows average score for each success factor.

Source: *Cross-border investigations: Are you prepared for the challenge?,* KPMG International 2013.

Just as cultural and language sensitivities matter in every other form of cross-border interactions, they also matter in investigations. While this sort of cross-border and cross-cultural sensitivity should be applied across all geographies, it is particularly relevant in certain countries with a history of governmental suppression. Accordingly, when conducting investigations in foreign jurisdictions, case managers and investigators should be mindful of the words they choose when dealing with foreign employees. For example, the word "investigation" may elicit negative emotions or connote a message that will have a chilling effect on the process. "Review," "analysis," or "discussion" are more impartial. Likewise, rather than saying "whistleblower," "informant," or "witness," term such as "employee" or "colleague" are neutral.

In addition to cultural differences, there are significant legal differences. Many countries have restrictive data privacy and labor laws that can significantly impact the scope and depth of an investigation. In certain countries, for instance, local law may require that internal investigations be disclosed to the government, particularly if the company is owned or controlled in any part by a government agency. Failing to modify investigatory practices when conducting cross-border investigations not only could be counterproductive from a cultural standpoint, it also could carry a consequence for an investigator – one that serves as an ironic book-end to what is often the focus of the investigation in the first place: a violation of law.

Case Study

A software company initiated an internal investigation of its Russian subsidiary. The investigators complied with Russia's strict limitations on removing data from the country and sent a team to Moscow to review all of the documents. As is common in the U.S., they encrypted the data not realizing that it is illegal in Russia to encrypt certain information. When the authorities learned about it, the investigation was delayed until the situation could be resolved. Knowing the local data laws could have prevented the issue.

© 2013 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

The following steps can assist case managers and investigators in handling cross-border investigations.

Assess the lead or allegation

When allegations involving international matters are made, the first step in the response protocol involves a preliminary assessment of the claim. "We learned as children to stop, look, and listen before crossing the street, and the same prudence should be applied before taking any action with regard to an allegation of misconduct," notes Déan Friedman, KPMG in South Africa. "Taking the time to assess the matter is critically important for the sake of confidentiality and privacy, as well as the credibility of the compliance program, the integrity of the investigation progress, and the reputation of those involved."

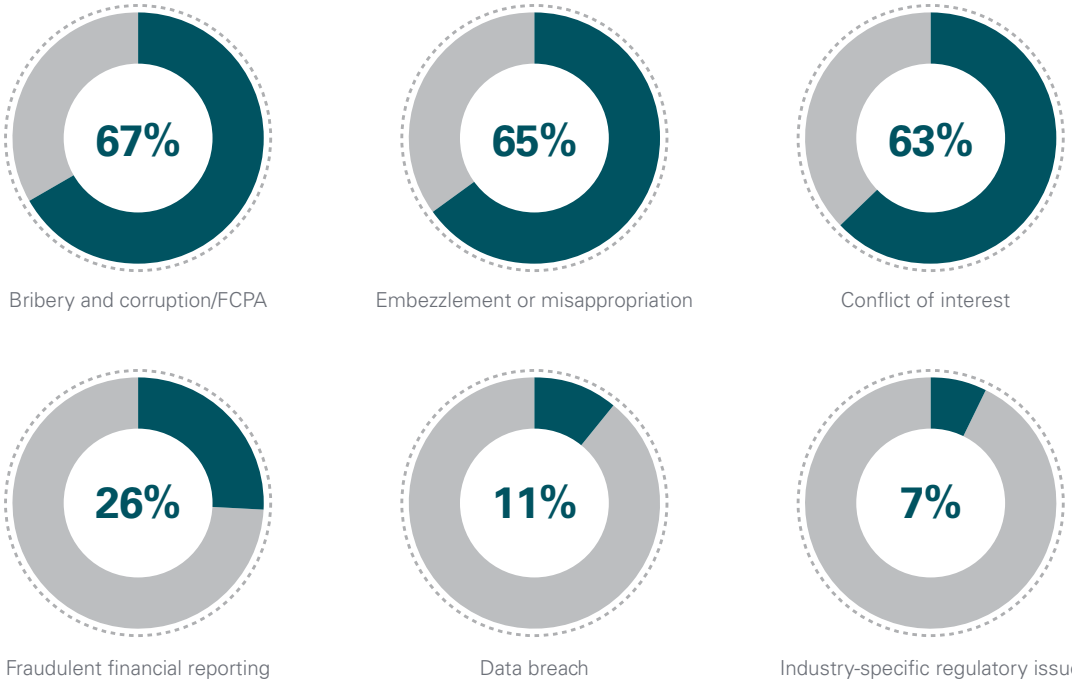
When assessing cross-border allegations, the compliance officer, lead investigator, or case manager should take the following steps:

- Understand the factual nature and substantive issues involved in the allegation;
- Pinpoint, to the extent possible, the geographic source of the allegation;
- Identify the laws and policies that may be relevant;
- Determine the pervasiveness of the potential wrongdoing;
- Evaluate the credibility of the allegation;
- Identify country-specific laws and cultural norms that may affect the investigative process;
- Determine whether additional subject-matter or local professionals are needed;
- Develop a preliminary time table and budget to administer and complete the investigation;
- Determine whether and how to communicate with the claimant; and
- Assemble an investigation team involving local team members who have cultural and language expertise.

Implement short-term action steps

Just as with domestic allegations, cross-border matters run the gamut, including employee relations concerns, corruption, data privacy breaches, theft, workplace violence, and so on. Case managers handling cross-border issues need to take certain preliminary steps to help protect the integrity of the process, employee safety, privacy and confidentiality, company property, and potential evidence. Depending on local law, such steps could involve temporarily suspending or placing on leave employees who are the subject of the concern or taking measures to preserve evidence and relevant documentation. Some countries also require notification to an employee who is the subject of an allegation, or to an employee representative or work council.

Which of the following best describes the nature of the cross-border investigations you are performing or managing?



Source: *Cross-border investigations: Are you prepared for the challenge?*, KPMG International 2013.

© 2013 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Develop a plan

All effective investigations, whether domestic or foreign, contain certain common elements. Before an investigation is launched, case managers should develop a plan that contains these steps outlined above. A thorough and well-designed plan can help investigation team members stay focused on the objectives of the investigation, measure progress along the way, and strategically incorporate supplemental steps as they become necessary. An investigation plan typically centers on a hypothesis that posits why and how the misconduct occurred. The plan should establish the scope and objectives for the investigation, the documents and data to be collected, the individuals to be interviewed, the timeline and milestones, and the reporting process.

In a cross-border context, the investigative team also needs to take into account any jurisdictional differences that may impact the investigation, the information that can be collected, and the individuals who can be interviewed. For instance, in certain European countries, due to personal data protection laws, the scope of an investigation involving an anonymous whistle-blower may be restricted. In China, many businesses are state-owned or controlled, which may trigger China's states secrets laws and greatly impact the kind of data that can be collected and reviewed. A well thought out plan should predict the kinds of issues that may arise and lay out a strategy to address them.

Determine who should be notified

An important early step in the case-management of cross-border investigations is to alert key members of management that a potentially significant compliance allegation has been filed and that an investigation will be initiated. Depending on the nature of the matter, it may be appropriate to notify the country manager, the functional leader, the department head, or other members of local management. It is important to keep the circle of trust small and to remind members of management about confidentiality and the integrity of the process. "We have seen instances where a member of the local country management is notified that an investigation is about to be launched, and then that person turns around and shares the news with the subject," reports Rachael Layburn, KPMG in China. Such sharing of information may be seen as violating basic investigatory practices, but in some countries it may be common practice. Knowing local customs and practices can help avoid an unintended disclosure.

Identify who will oversee and conduct the investigation

Allegations vary in substance, severity, and priority. Therefore, a company should have a detailed procedure or protocol that outlines which department or individuals will bear responsibility for overseeing the investigation. "It is vital to have all the critical stakeholders at the table early to agree to the work plan and to set communication protocols at the very beginning," advises Pam Parizek, KPMG in the US. "When an investigation is being conducted overseas in different time zones, it creates challenges to keeping these stakeholders informed in a timely manner." The protocols, therefore, need to include not only the planned investigative procedures, but also the channels of communications with those overseeing the investigation.

While the legal department would likely oversee investigations involving potential legal matters, human resources may oversee investigations related to employee-relations issues, theft, and physical security. Moreover, potentially significant compliance situations, including those that involve serious violations of domestic or foreign law, fraudulent financial reporting, or senior management would require direct board or audit committee oversight. These oversight groups should help establish the scope of the investigation, review the investigation plan, and ensure that adequate resources are available.

"The oversight group plays an important role with regard to the framework of a cross-border investigation," notes Maurice L. Crescenzi, Jr., KPMG in the US. "It is critically important that those who oversee and manage the investigation become intimately familiar with the local business and its operations, while at the same time, understanding the legal and cultural environment." In some instances, hiring local outside counsel to handle the investigation is appropriate. However, the outside law firm should be an independent firm and not the company's regular counsel in the jurisdiction.

Many companies struggle with the unique challenges of staffing a cross-border investigation. More than forty percent of respondents in KPMG's survey believe that their companies lack sufficient resources to handle cross-border investigations. Individuals need not only to be experienced in investigative strategy and tactics, but they also must understand local law, language, and customs. Investigation teams who do not have local language skills may miss critical aspects of key documents or interviews conducted in local language. "I can't stress enough the importance of having members of the investigations team who understand local culture and local language," says Crescenzi. "You simply cannot conduct a cross-border investigation using people who do not know the intricacies and idiosyncrasies of certain jurisdictions." These individuals may be hard to come by, and companies need to be prepared before a need arises.

© 2013 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Case Study

Amid allegations of employee fraud at an international joint venture in Taiwan, a global consumer products company realized that it did not have the resources to respond immediately. The matter was exceedingly sensitive because of the stature of the subject and family-ownership of the joint venture. For assistance, the company retained a firm that had familiarity with the local business environment and culture, and had experience with Taiwanese law enforcement. The investigation was conducted in way that respected the sensitivities and resulted in a criminal prosecution.

To be well prepared, companies with global operations should proactively train employees about investigation protocols in different jurisdictions so that they can respond quickly. Trying to educate local resources after an allegation has been received may lead to delays that can sidetrack an investigation. Yet only thirty-five percent of respondents in KPMG's survey said that their companies conduct investigations training each year. Unlike domestic investigations, cross-border investigations oftentimes require specialized staffing that necessitates proactive planning. Companies can address gaps in resources by developing contingency plans for investigative personnel, such as designating experienced internal people from other regions to respond if necessary, and retaining outside local investigators to be on call when a situation arises.

Assess special legal or cultural considerations

Both domestic and international investigations almost always involve data collection, interviews, and other sensitive communications. For this reason, attorney-client privilege and the attorney work product doctrine are important considerations. Attorney-client privilege protects confidential information disclosed to an attorney in the process of obtaining legal advice or assistance. In contrast, the attorney work product doctrine, which is broader, applies to tangible material or its intangible equivalent collected or prepared in anticipating of litigation or a trial, which extends to the investigative process. Before a company launches an investigation, it should consult with in-house or external counsel familiar with the law of the relevant jurisdiction as to whether the investigation can be privileged or protected.

In an international setting, local law also may limit the scope of the investigation. For instance, in Europe an investigation into an anonymous complaint cannot be as broad as an investigation in which the allegation is made by an identified employee. Wherever possible, case managers and investigators, through their secure and confidential internal case-management systems, should attempt to have an anonymous claimant identify himself or herself. In some jurisdictions, it can be illegal for companies to investigate alleged employee misconduct because the local government considers itself to be the exclusive investigator responsible for law enforcement. Here again semantics matter. If management refers to the activity as a "review" rather than an "investigation" it could make a legal difference.

Lastly, case managers and investigators should be sure that the scope of their investigative plan includes a review of whether the subject violated local law. While it is not uncommon for many companies to predicate their global standards and compliance policies on their domestic laws, cross-border investigators should also evaluate whether local law, too, has been violated. Many times, these laws are not in alignment.

© 2013 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

04 Conducting a cross-border investigation

The manner that investigative procedures are implemented and the legal framework in which they are governed can differ dramatically from country to country. Companies involved in cross-border investigations are faced with navigating a variety of foreign laws and regulations that, in many respects, change the way an investigation can be conducted. "Local legislation may significantly influence the manner in which investigations are planned and executed," notes Jimmy Helm, KPMG in the Czech Republic. For example, in certain jurisdictions the mere observation of conduct, such as the weighing process at weighbridges or truck scales, may be regarded as an infringement of privacy. "More invasive procedures such as reviewing an individual's emails or confrontational interviews may be greatly limited," Helm says.

Cultural differences also underlie cross-border investigations and can create significant problems if investigators do not understand and respect these differences. "In cross-border investigations, it is important to understand the traditional culture that is driving how people think, act, and react, and how the person conducting the investigation is being perceived," says Shelley Hayes, KPMG in Mexico. What may be acceptable to say or do in one culture may totally offend someone from another culture. "Loyalties also differ by culture and some employees may be hesitant to speak out against a countryman for the benefit of a foreign company," explains Mark Leishman, KPMG in Australia. It comes as no surprise that more than a third of the respondents in KPMG's survey identified cultural differences among their top challenges in cross-border investigations.

Proactively identifying and addressing legal and cultural differences is the key to conducting an effective cross-border investigation. In our experience, significant differences between cross-border investigations and domestic investigations include data privacy laws and regulations, interviewing employees, and reporting findings.

Case Study

Certain local laws that provide a right to access public information could result in a third party's obtaining a copy of your confidential report. The operator of an Italian railway, which was partially owned by Italy's Ministry of Economy and Finance, was required to report the findings of an accounting investigation to the Ministry and its designees. The report harshly criticized the chief accountant, causing him to lose his job. Because the report had been disseminated to others, he could not find employment in the industry. He brought a lawsuit for defamation against the company. If the company had realized that the report might not remain confidential, it might have been written in a manner that would not have exposed it to a potential claim.

© 2013 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

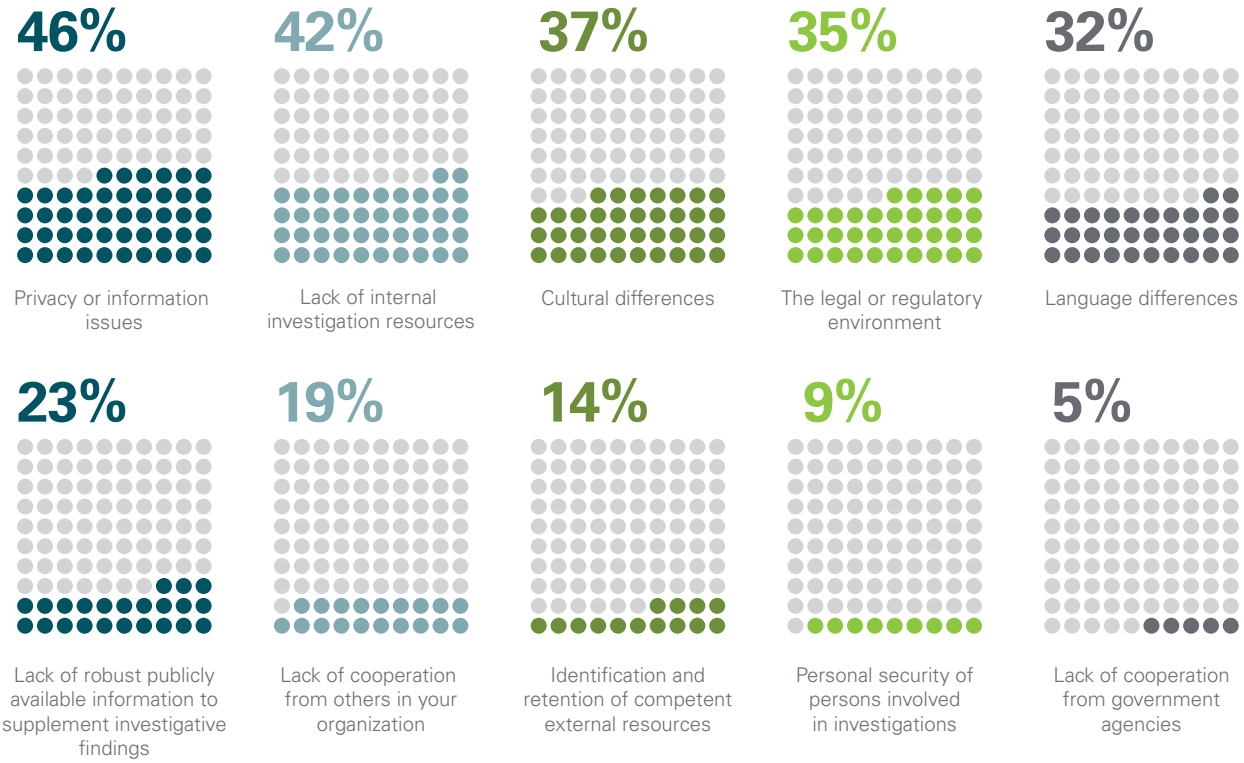
Data privacy

Preserving and collecting information relevant to an investigation is one of the most important steps in the investigative process. Foreign data privacy laws and regulations pose some of the greatest challenges to conducting cross-border investigations because of restrictions on the kinds of data that can be collected and transferred out of the jurisdiction. Many countries have enacted laws that place a high priority on protecting personal data, including establishing a fundamental legal right on the privacy of personal data, even if such data are contained on an employer's system or computer. In fact, over forty six percent of the respondents in KPMG's survey reported that their greatest challenge in conducting cross-border investigations is handling data privacy issues. "Being sensitive to data privacy and regulations in individual countries is a fact of life in cross-border investigations," says Rocco deGrasse, KPMG in the US. "You cannot, for example, conduct an investigation in the European Union, or especially in China, without first understanding what legal limits are placed on collecting and exporting data."

Failing to anticipate the impact of local data protection laws not only can significantly impede an investigation, but it also can be costly in terms of added expenses, sanctions, and, in some cases, prosecution. For example, China has strict laws that prohibit the collection, review, and transfer of "state secrets" and other information that is in China's national interest. However, China's laws do not define what are state secrets or national interests. Because China is highly controlled and managed by the State, most companies operate with an abundance of caution by keeping as much information within China's borders and by hiring local experts who are intimately familiar with the risks of violating China's laws.

The data privacy laws of some countries may prohibit a company from reviewing certain data in a company's own files unless the data originally was obtained for investigatory purposes, which many times is not the case. One of the biggest hurdles is complying with limitations on collecting and reviewing data in a company's readily-accessible files, such as emails on the company's server, internet use records, documents on an employee's hard drive, and even hard copy documents in an employee's office. This is a formidable challenge. Indeed, the respondents in KPMG's study believe that the most difficult task in cross-border investigations is gathering relevant information, especially electronic data.

Which of the following are the top 3 challenges your company faces in the course of conducting cross-border investigations (select up to 3)?



Note: Chart shows the number of participants who chose the specified challenge as a percentage of total participants who responded.

Source: *Cross-border investigations: Are you prepared for the challenge?*, KPMG International 2013.

© 2013 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Unlike a common presumption in some countries that a company has the right to search data on company-owned systems and computers, the prevailing view in many foreign countries is that personal data is protected regardless of where it is stored. "Most jurisdictions in Central and Eastern Europe require the approval of the person before their email accounts may be extracted and interrogated as part of an investigation," says Jimmy Helm, KPMG in the Czech Republic.

The model for many foreign data protection laws is European Union Directive 95/46/EC, the primary legislation to date on data protection in Europe. The EU Directive broadly defines personal data as "any information relating to an identified or identifiable natural person." It restricts the collection and processing of personal data to limited circumstances such as when the individual has consented, when it is necessary to comply with a legal obligation, or when a legitimate corporate interest is not overridden by the fundamental rights and freedoms of the individual. These situations are not always clear, and foreign regulators may have varying opinions as to their applicability.

Obtaining relevant data, however, is only the first step. "One has to understand whether there are restrictions on taking data out of the local country," explains Roy Waligora, KPMG in South Africa. Many foreign data privacy laws, including those in Europe and parts of Latin America and Asia, prohibit transferring data out of the local jurisdiction without first establishing data export channels. Data export channels are methods of ensuring that country-specific data protection procedures will be followed, such as adopting corporate policies that adhere to foreign data protection laws; incorporating model contract clauses that provide a "safe harbor" under laws like the EU Directive; and, in some cases, obtaining consents by employees. It is vitally important to establish these data export channels *before* an investigation arises to prevent delays or roadblocks in a cross-border investigation.

Another important difference between domestic and foreign data privacy laws relates to the confidentiality of investigation materials. Many countries require that investigators disclose personal data included in investigation materials to the individuals who are targets of the investigation if they request the data. Additionally, labor laws in some countries may require companies to disclose investigatory procedures involving data processing systems to labor unions or employee rights work councils if personal data could be impacted. "Balancing the integrity of the investigative process with the legal rights that overseas subjects enjoy under local law is both an art and a science," says Tim Hedley, KPMG's Global Leader for Fraud Risk Management. "One way to strike this balance is to wait for an appropriate time in the investigative process to share this information once the investigation is mature and the findings have begun to take shape."

Case Study

A US company initiated an investigation of certain of its overseas operations in Europe. The company had a global policy that it could review emails that were contained on company-owned computers and systems. In accordance with its policy, the company copied the emails of a number of foreign employees. However, when investigators tried to leave the country with the copies of the emails, the data was confiscated by a customs official until the company could provide consents from each employee. This led to significant delays because some of the employees initially refused to consent, while others could not be located. Creating export channels beforehand, such as getting consents, could have prevented the situation.

Important differences in data privacy laws can have an impact after the conclusion of a cross-border investigation. Some countries prohibit outdated personal information from being retained, even if it is contained in investigatory materials. This runs counter to certain laws and regulations that may require a US company to maintain investigatory materials and work product for a period of time. "Having a solid understanding of the data privacy laws in the jurisdiction is critical from the beginning through the end of a cross-border investigation. In most cases, this means relying on experts who have in-country experience with handling data," says Ken Koch, KPMG in the US.

Interviewing employees

Interviewing employees who are located in a foreign country raises unique legal and cultural issues that oftentimes are fraught with pitfalls. In many countries, employees have the right to refuse to cooperate with an employer-led investigation, even if they are not its target. For example, in some jurisdictions, including Europe, rules prohibit employers from requiring their employees to report incriminatory information about co-workers. Labor laws in many countries mandate that an employee representative or union committee be consulted before an employer may interview its own employees in an investigation. One of the starkest differences between domestic and cross-border investigations is the requirement that companies in some countries have to inform their employees of procedural rights during the investigation and give them at least some degree of access to investigation materials that identify them. Employees also may have the right to have a lawyer or employee representative present at the interview.

Understanding local culture plays a pivotal role with interviewing employees in cross-border investigations. "In some cultures, talking about fraud, theft, and manipulation of financial statements is accepted; in others, the same words will put people on edge," observes Shelley Hayes, KPMG in Mexico. Even body language may differ. "Looking someone in the eye is considered rude in some countries, so it should not be taken as

© 2013 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

a clue that a person is lying if he or she does not maintain eye contact with an investigator," notes Mark Leishman, KPMG in Australia. Conducting an interview in a confrontational manner may be effective, but in many countries, the interviewing style needs to be softened. These kinds of insights are relevant to cross-border investigations and investigators should be mindful of what it will take to put a witness at ease during an interview.

Language differences can pose problems at every stage in cross-border investigations, and they may be most acute when interviewing witnesses. Unlike documents that are written in a foreign language, witnesses oftentimes speak with different dialects, or use slang or local jargon. Some spoken words and terms also do not translate in exactly the same way between languages. It is no wonder that language differences were ranked as a top challenge in cross-border investigations by nearly a third of the respondents in KPMG's survey. Using investigators with local language skills, particularly those having the appropriate regional dialects, can be essential when interviewing witnesses. When different languages are involved, another area that poses a high risk is obtaining an accurate translation of an interview into English. Even slight variations in translations could create significant misinterpretations of the reported facts.

Reporting findings

Careful attention should be paid to the form and content of a report in a cross-border investigation. There may be advantages to providing only an oral report, but the labor laws in a particular jurisdiction may require a written report, especially if disciplinary action is taken. Many countries have data privacy laws that allow a target or a witness to have access to certain investigatory material, including a written investigation report. Being compelled to disclose data in this way could affect the applicability of domestic and foreign legal privileges and could expose the company to data privacy and defamation claims.

Case Study

During an internal investigation in a European Union member state, the company's employee rights council intervened on behalf of an employee, in part because the company had not notified the council that it was going to collect the employee's data. The council claimed that the data included personal data and it threatened to get a court order to halt the investigation. The resulting publicity could have threatened the confidentiality of the investigation. The company ultimately agreed to segregate any personal information and disclose it to the employee and to the council before including it in any investigation materials. This increased the costs of the investigation and caused delays. Working with the council proactively could have avoided the delays.

A company needs to keep in mind that an investigation report may contain data that is restricted from being transferred out of a jurisdiction, such as names of individuals, financial information, or personal data. Therefore, the proper data export channels need to be established before providing a report (even a report in draft form) to management or directors outside of the country. These considerations apply likewise to reports and materials prepared by experts and consultants. "A company conducting a cross-border investigation needs to make sure that all of its outside experts and vendors who receive data comply with local data privacy laws," advises Jack DeRaad, KPMG in the Netherlands. "This can be challenging when there are many experts involved, such as lawyers, forensic accountants, ediscovery vendors, and computer forensic specialists, especially if they are located in various jurisdictions with different data privacy regimes."

An understanding of local law is critical in reporting the findings of a cross-border investigation. The data privacy laws of some countries restrict an employer from reporting to enforcement authorities the personal information found during an investigation. In contrast, other countries, such as Australia, require an employer with evidence of certain criminal offenses to report them to police. It is easy to see how conflicts might arise between the reporting restrictions and requirements of different jurisdictions. Knowing beforehand if reporting restrictions exist can help to avoid difficult situations at the conclusion of a cross-border investigation.

Case Study

An employee in India who was being interviewed by a company's U.S. investigator claimed that she was intimidated and harassed because the investigator emphasized that he formerly was a federal prosecutor and that the company would take criminal action against anyone found guilty of wrongdoing. The harassment claim interrupted the investigation and caused the employee to refuse to cooperate. Understanding local culture and practices might have changed the way in which the investigator approached the employee.

© 2013 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

05 Remediation across borders

Once the fact finding stage of a cross-border investigation is complete, a company may need to remediate any issues identified, which could include correcting books and records, fixing control weaknesses, and disciplining employees. Taking remedial action can be an important determinant by regulators, both domestic and foreign, in deciding to charge a company with a violation of a law or to reduce the size of a criminal fine or penalty that might be assessed. Remediation across borders, however, can create unsuspecting challenges.

One of the first considerations is how to handle employees found to have engaged in wrongdoing. These employees may have different levels of culpability and may be located in jurisdictions with different legal or labor protections against adverse action. While it is critical that companies punish employees proportionately to their role in the misconduct, it also is important to follow local regulations when doing so. For instance, certain countries require employers to first notify an employee if he or she is going to be terminated for cause. And in some places, such as Austria and Belgium, this notification may need to be made within days of obtaining evidence of wrongdoing.

While the kinds of punishment can run the gamut, terminating an employee could trigger different requirements in different jurisdictions. "Even if an employee is being terminated for cause, you have to be careful to follow local dismissal procedures," advises Mike Schwartz, KPMG in the US. "The first reaction may be to fire a guilty employee as soon as possible, but that could violate local laws or employee rights." Even if the evidence appears to implicate a person, the labor laws in some countries contain high standards that must be met in order to justify a termination for cause. Domestic and foreign regulators also may complicate matters by requesting that a company not terminate a culpable employee so that the regulator continues to have access to the employee. Even in this situation, a company should change the responsibilities of the affected employee to make sure he or she cannot repeat past misdeeds or be put in a position with a comparable level of authority, which could be interpreted as insufficient punishment.

Another key area of remediation is to adequately address the deficient, insufficient, or ineffective controls or procedures that allowed the misconduct to occur or to avoid being detected. In a multi-national company, these controls and procedures need to be examined not only in the affected location, but also wherever they exist globally, and they need to be remediated if necessary. While regulators may be impressed with the overall level of effort, they, along with management and directors, may insist on an interim fix to the controls that provides assurance that some remedial action is occurring while a longer term solution is being implemented. Keep in mind, however, that in some countries there may be limitations on the ability of an employer to make substantive changes to the work environment without consulting labor unions or workers' councils.

The timing of remedial action also is a consideration. Oftentimes, remediation can and should begin as soon as inadequate or compromised financial controls have been identified, even during the investigative fact finding. "Both the board of directors and the regulators will expect, or at least welcome, prompt attention to fixing known gaps, workarounds, or weaknesses in compliance protocols or financial controls without waiting for the investigation to be completed," advises Rocco deGrasse, KPMG in the U.S. In a complex matter, remediation of multiple controls across multiple countries may take a long time, even years. "Law enforcement and regulatory authorities may be reluctant to finally resolve regulatory and other proceedings until they know the company has fixed the gaps in all affected countries and has taken some sort of action against responsible employees," says Charlie Patrick, KPMG in the UK. "The bottom line with conducting remediation across borders is to start promptly and to proceed prudently."

© 2013 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

06 Concluding remarks

Given the challenges created by cross-border investigations, ninety-five percent of the respondents in KPMG's survey expected that their needs for cross-border investigations will increase or at least to stay the same over the next year. Add to this, the increase in global regulations, laws, and enforcement actions, companies with well designed cross-border investigation protocols will be positioned for more positive outcomes than those that are not prepared. At each stage of a cross-border investigation, there are unique challenges that require forethought and planning to manage the risks and to respond swiftly and appropriately. No longer can companies rely on procedures and resources used for domestic investigations. Instead, they must be customized to comply with different local laws and to respect diverse cultures and customs. When allegations can arise from almost anywhere around the world, at any time around the clock, and in virtually any language, every company should answer the question: Are you prepared for the challenge?

We would like to acknowledge the following individuals for their assistance:

Laura Alderson
Nina D'Arcangelo
William Hanley, III
Jilane Khakhar
Victoria Malloy
Lissa Mitchell

Special aknowledgement to Scott Hilsen for his significant contributions in helping with the successful completion of this project.

Contributors

Maurice L. Crescenzi Jr.
KPMG in the US
T: 973 912 4861
E: mcrescenzi@kpmg.com

Rocco de Grasse
KPMG in the US
T: 312 665 1296
E: rdegrasse@kpmg.com

Shelley Hayes
KPMG in Mexico
T: +52 5552468634
E: hayes.shelley@kpmg.com.mx

Jimmy Helm
KPMG in the Czech Republic
T: +42 0222123430
E: jhelm@kpmg.cz

Timothy Hedley
KPMG in the US
T: 212 872 3496
E: thedley@kpmg.com

David Hicks
KPMG in the UK
T: +44 20 76942915
E: david.hicks@kpmg.co.uk

Scott Hilsen
KPMG in the US
T: 404 222 3015
E: shilsen@kpmg.com

Ken Koch
KPMG in the US
T: 404 614 8658
E: kckoch@kpmg.com

Rachel Layburn
KPMG in China
T: +86 108 5087075
E: rachel.layburn@kpmg.com

Marc Miller
KPMG in the US
T: 212 872 6916
E: marcmiller@kpmg.com

Charlie Patrick
KPMG in the UK
T: +44 20 76945470
E: charlie.patrick@kpmg.co.uk

Pamela Parizek
KPMG in the US
T: 202 533 5362
E: pparizek@kpmg.com

Alex Plavsic
KPMG in the UK
T: +44 20 73113862
E: alex.plavsic@kpmg.co.uk

Mike Schwartz
KPMG in the US
T: 713 319 2258
E: mschwartz@kpmg.com

Roy Waligora
KPMG in South Africa
T: +27 736222319
E: roy.waligora@kpmg.co.za

© 2013 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Contact us

KPMG's Global Forensic Investigations Network

Phillip Ostwalt
Global & Americas Leader
T: 404 222 3327
E: postwalt@kpmg.com

Dean Friedman
EMA Leader
T: +27 116478033
E: dean.friedman@kpmg.co.za

Mark Leishman
AsPAC Leader
T: +61 7 3233 9683
E: mleishman@kpmg.com.au

KPMG's Global Forensic Regional Leadership

Petrus Marais
Global Forensic Leader
T: +27 795159469
E: petrus.marais@kpmg.co.za

Richard H. Girgenti
Americas Region Forensic Leader
T: 212 872 6953
E: rgirgenti@kpmg.com

Jack DeRaad
EMA Region Forensic Leader
T: +31206 567774
E: deraad.jack@kpmg.nl

Grant Jamieson
AsPAC Region Forensic Leader
T: +85 221402804
E: grant.jamieson@kpmg.com

kpmg.com/socialmedia

kpmg.com/app

Available on the App Store

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.
The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International. NDPPS 225200

Designed by Evalueserve.

Publication name: Cross-border investigations report

Publication number: 121643