



FORENSIC

Cross-Border Investigations Effectively Meeting the Challenge

ADVISORY

Contents

Introduction and Executive Summary	1
Current Environment	2
Defining Fraud and Misconduct	5
Taking the Appropriate First Steps	6
Meeting the Challenge of Taking the Appropriate First Steps	8
Cultural and Legal Differences	10
Meeting the Challenge of Cultural and Legal Differences	12
Resources	14
Meeting the Challenge of Resources	16
The Availability and Accessibility of Electronic Data	18
Meeting the Challenge of Availability and Accessibility of Electronic Data	22
Key Points to Remember	24

Survey Methodology:

Quantitative

- Conducted in November/December 2006
- Total respondents: 103
- Respondents: The most senior people in charge of day-to-day corporate investigations for their companies

Qualitative

- Thirty in-depth interviews with senior executives

Respondent Locations:

Argentina	Denmark	New Zealand
Australia	France	South Africa
Austria	Germany	South Korea
Belgium	India	Spain
Brazil	Italy	Switzerland
Canada	Japan	United Kingdom
Chile	Netherlands	United States of America



Introduction and Executive Summary



At a time when money and intellectual property can be digitally flashed in a matter of seconds across continents in the course of

global trade, the difficulty of preventing, detecting, and responding to international cross-border fraud, corruption, and misconduct is hard to overstate. The growth and the scale and sophistication of fraud and misconduct perpetrated against businesses around the world is accelerating. The negative impact in terms of lost revenue and property can be substantial – personal and business reputations, market capitalization, and investor confidence can all be rapidly and significantly impaired. What's more, when a business must respond to fraud and misconduct its management is distracted from focusing on growing and developing the business.

During the latter half of 2006 and early in 2007 KPMG, along with the research firm Penn, Schoen and Berland Associates Inc. approached multinational businesses in diverse industries around the world, and asked those charged with the responsibility for cross-border investigations within those companies how they responded to their current challenges.

As trade barriers fall and international commerce expands, and as the speed of conducting business and remitting funds increases, companies that conduct business across international boundaries are recognizing the corresponding increase in the risk of fraud and misconduct. However, it is clear from our research that some are more prepared than others. Those organizations have bolstered their cross-border investigations capabilities either through adding in-house resources or by forming alliances with a third party, particularly in the more specialized areas such as electronic data capture and review and data analysis.

An effective cross-border investigations capability is just one element in a comprehensive approach to risk management and investigation of fraud and misconduct. An effective approach can:

- Lower the risk of the occurrence of fraud or misconduct, thus lowering the possibility of being hit with serious sanctions
- Demonstrate to regulators, shareholders, stakeholders, bond-ratings agencies, and the capital markets that the business takes accountability and control seriously, thereby mitigating damage to reputations
- Exhibit the business's commitment to overall corporate governance activities
- Assist in a rapid and efficient response before issues spiral beyond control.

As part of our survey and follow-up interviews with senior business executives with responsibility for investigations, KPMG learned that the challenges in cross-border investigations faced by these professionals generally fell into four categories:

- Taking the appropriate first steps
- Cultural and legal differences
- Investigation resources
- The availability and accessibility of electronic data.

Our purpose in publishing this report is not only to describe those challenges in some detail but also to provide insights into possible responses to them. With that insight as background, we hope companies will be able to derive the best value for their current or pending investment in cross-border investigations, regardless of whether those are conducted in-house or undertaken with a third party.

Furthermore, an effective cross-border investigations plan demonstrates not only an organization's sound risk management practices, but also its overall commitment to good corporate governance.

We also believe this is the right time to engage in dialogue for the purpose of change and improvement.

Adam Bates
Global Chairman
KPMG Forensic

Current Environment

“One thing is clear...as international communications, the internet, and global commerce continue to expand, the internationalization of fraud investigations will increase apace...”

Seth T. Taube, partner and Chief of the Trial Section of the New York office of Baker Botts LLP, and author of *Investigating Foreign Subsidiaries: The Mixed Marriage of Alien Cultures and Domestic Laws*, American Conference Institute, March 1, 2006



“The risks to companies from corruption are growing and the effects of corruption are especially severe on transition economies. Our review has shown that reporting is improving among best practice companies, most often those at greatest risk from corruption, but for the majority of companies the issue is still handled in a low profile manner. TI [Transparency International] strongly encourages companies to improve their reporting to support their reputation for integrity.”

David Nussbaum, Chief Executive
Transparency International

A global airline based in Asia belatedly discovers a travel agent operating in a number of countries uses its reservation system to steal at least USD5 million. An international energy concern based in Africa learns that one of its executives illegally diverts some of its product from one country to a business in which he owned an interest that is located in another country. A financial services company based in Europe unearths a massive multi-nation, money-laundering scheme operated by a crime syndicate that threatens its reputation. The list goes on and on, with similar stories and new twists.

For senior management and board members around the world, the above examples of fraud and misconduct are not surprising. Yet, the speed with which these cross-border crimes are committed appears to be increasing, fueled by the rapid advances in both global trade and information technology. Consider this comment made by an Asia-based transportation-industry senior executive in our recent survey: “...Continued advancement in the area of IT [information technology] has made it so much simpler for the crooks to defraud us....International boundaries don't affect the criminals, and IT issues don't affect criminals, but they certainly affect us.”

The argument could be made that because global forces are driving businesses to operate in certain countries where there are lax or seldom-enforced laws regarding, for example, bribery and corruption, the need for robust cross-border investigative capabilities will continue to increase.

Furthermore, a company's ability to respond to the increased sophistication and speed of perpetration of fraudulent

acts and subsequent rapid distancing of funds and assets has generally not kept pace with the speed and increased sophistication of fraud.

At the same time, the need for effective cross-border investigations is also being driven by ever-more stringent regulatory directives in many countries. Some examples of currently enacted laws and regulations are:

- In the United States: the Foreign Corrupt Practices Act (FCPA), the USA PATRIOT Act, and the Sarbanes-Oxley Act of 2002, section 404.
- In the United Kingdom:
 - The Anti-Terrorism, Crime and Security Act 2001 includes extra-territorial provisions relating to corruption.
 - The Proceeds of Crime Act 2002 permits recovery of assets in the United Kingdom that are the proceeds of an act committed outside the United Kingdom and that are both illegal in the country where committed and in the United Kingdom.
- In Australia: the Commonwealth Criminal Code Act 1995 makes it an offense to bribe a foreign public official, whether in Australia or in another country.
- In Canada: the Corruption of Foreign Public Officials Act.
- In Germany: The Federal Government Directive Concerning the Prevention of Corruption, 2004, sets the legal framework for enacting the federal government's corruption prevention strategy and includes an anti-corruption code of conduct. The existing German penalty code and criminal procedure law allows the pursuit of employees of foreign companies if they are involved in corrupt activities while in Germany.

- In South Africa: The Prevention and Combating of Corrupt Activities Act No. 12 of 2004 provides for the strengthening of measures to prevent and fight against corrupt activities.
- The Organisation for Economic Cooperation and Development (OECD) Anti-Bribery Convention. According to its newest ratification list, the OECD's Anti-Bribery Convention has been implemented in 36 countries as of November 2005. This number includes most of the countries within the European Union.

Some examples of emerging, pending, and evolving laws and regulations are:

- In the United Kingdom: The Proceeds of Crime Act 2002 is a developing area with other Bills before Parliament that if enacted in their current form will codify or impact the Act further.
- In Germany: Reportedly under consideration is the introduction of legislation tightening anti-corruption law,¹ which is the result of recent corporate scandals. The legislation reportedly would increase public prosecutors' power to investigate corruption of a broader range of implicated employees.
- In China: Laws passed by the National People's Congress, including the Criminal Law and the Anti-Money Laundering Law currently being enacted, set the rules for anti-money laundering requirements for financial institutions with banking functions, and clearly establish the basic framework for anti-money laundering reporting and information monitoring systems.

Participants in the Association of Certified Fraud Examiners' 2006 National Fraud study estimate U.S. organizations lose 5 percent of their annual revenue to fraud. Applied to the estimated 2006 United States Gross Domestic Product, this 5 percent figure would translate to approximately USD652 billion in fraud losses, according to the 2006 ACFE Report to the Nation on Occupational Fraud & Abuse.

There is also in existence a United Nations Convention against Corruption that was entered into force in December 2005, after countries worldwide were provided the opportunity to sign it. The Convention sets measures dealing with corruption with respect to its prevention, criminalization, international cooperation, and asset recovery.

To be effective against the threat of fraud, corruption, and misconduct, multinational organizations must continually assess their cross-border investigative capabilities – as well as their overall fraud risk management programs – in order to ensure the right balance is struck among their efforts regarding the prevention, detection, and response to fraud and misconduct.

Though determining the specific financial impact of cross-border fraud and misconduct has proved very difficult for law enforcement organizations around the world, there is no doubt about the scope and nature of these corrosive crimes. "National borders rarely prove to be barriers to determined fraudsters," according to the Serious Fraud Office in the United Kingdom.² "Money is channeled through overseas banks and offshore companies, victims can reside anywhere in the world, and suspects and evidence can hide behind the laws of different jurisdictions." And, therein lie the aspects of cross-border fraud and misconduct that often differentiate them from other types of occupational fraud that a business may face. The investigation of cross-border fraud and misconduct frequently involves numerous legal issues, jurisdictions, and cultural challenges. As a result, businesses often are faced with resource constraints due to the geographic considerations of a cross-border investigation.

"...bribery of foreign government officials in international business transactions is a serious threat to the development and preservation of democratic institutions. Not only does it undermine economic development, it also distorts international competition by seriously misdirecting resources. Each country must adopt the necessary national legislation to criminalize the bribery of foreign public officials and address related obligations under the Convention. Examples of such obligations include insisting on corporate responsibility for the offence, sanctioning the laundering of the bribe and the proceeds of foreign bribery, penalizing related accounting omissions and falsifications, and providing mutual legal assistance and extradition."

From The Organisation for Economic Co-operation and Development's Web site (http://www.oecd.org/about/0,2337,en_2649_34177_1_1_1_1_1,00.html)

Consider some of the key challenges reported by survey respondents:

- Roughly half said their company does not have comprehensive protocols covering investigation processes
- Identifying/scoping the allegation presents a significant challenge
- Most do not have a dedicated function for managing cross-border investigations
- Many do not have ready access to the right levels of skills and resources – internally or externally – in order to conduct an effective cross-border investigation
- The availability and accessibility of electronic data presents a serious challenge

¹ Jurist, Legal News and Research, University of Pittsburgh, Jan. 14, 2007, <http://jurist.law.pitt.edu/paperchase/2007/01/germany-to-toughen-anti-corruption-law.php>

² <http://www.sfo.gov.uk/international/international.asp>

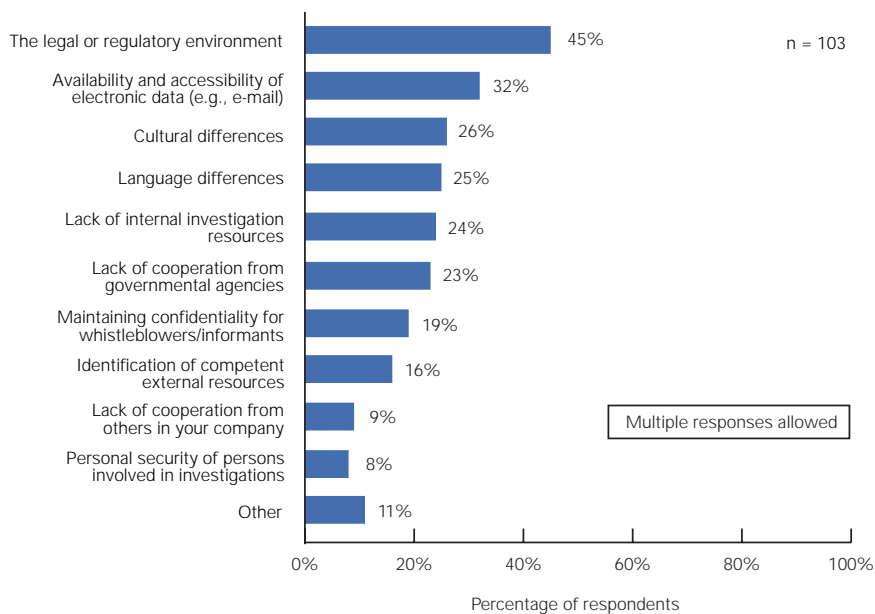
Respondents identified the following primary drivers of success for an international or cross-border investigation

- Proper planning and identifying the scope, 56 percent
- Effectively utilizing internal resources (including people and technology), 40 percent
- Hiring the right external resources, 34 percent
- Communicating effectively, 32 percent
- Managing expectations of senior management, 27 percent
- Coordinating with government or local authorities, 17 percent

- Companies say they find it challenging to stay current with laws on the gathering, storing, and transporting of data
- Four of the top six challenges in conducting cross-border investigations deal with cultural and legal differences
- Ninety-two percent of respondents expect cross-border investigations to continue at the current pace or to increase.

When discussing the critical challenges they face in cross-border investigations, the primary concerns of executives in our survey fell into four broad categories, including those dealing with the first steps, cultural and legal differences, resources, and the availability and accessibility of electronic data. Consequently, we have organized our report around these findings and included some ideas on how to handle them.

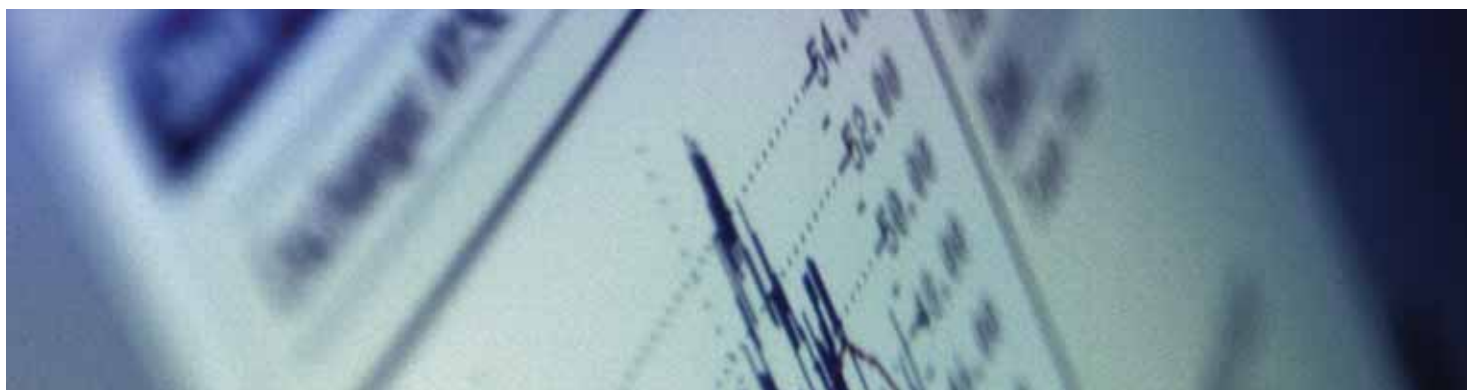
Top challenges in conducting cross-border investigations



Source: KPMG International, 2007



Defining Fraud and Misconduct



Fraud is a broad legal concept that generally refers to an intentional act committed to secure an unfair or unlawful gain.³ Misconduct is also a broad concept, generally referring to violations of laws, regulations, internal policies, and market expectations of ethical business conduct. Together, they fall into the following categories of risk that can undermine public trust and damage a company's reputation for integrity:

- Fraudulent financial reporting (e.g., improper revenue recognition, overstatement of assets, understatement of liabilities)

International Standard on Auditing 240 (ISA 240) on fraud:

The term "fraud" refers to an intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage.

- Misappropriation of assets (e.g., embezzlement, payroll fraud, external theft, procurement fraud, royalty fraud, counterfeiting)
- Revenue or assets gained by fraudulent or illegal acts (e.g., overbilling customers, deceptive sales practices, accelerated revenue, bogus revenue)
- Expenses or liabilities avoided by fraudulent or illegal acts (e.g., tax fraud, wage and hour abuses, falsifying compliance data provided to regulators)
- Expenses or liabilities incurred for fraudulent or illegal acts (e.g., commercial or public bribery, kickbacks)
- Other misconduct (e.g., conflicts of interest, insider trading, discrimination, theft of competitor trade secrets, antitrust practices, environmental violations)

Scandals and failures, together with flourishing and cynical greed may have profound and prolonged effects on public opinion. It is our collective duty and well-understood interest to demonstrate that market economy goes together with integrity and common good.

Black's Law Dictionary (Eighth Edition, 2004) defines misconduct as a "dereliction of duty; unlawful or improper behavior." Further, it is defined as "an affirmative act of misrepresentation or concealment of a material fact; intentional wrongful behavior"

³ *Black's Law Dictionary*, Eighth Edition, Bryan A. Garner, Editor, West Group, 2004

Taking the Appropriate First Steps

Identifying and scoping the initial steps to respond to an incident of alleged fraud or misconduct can increase the chance that the cross-border investigation results in a positive outcome. The need for an investigation arises suddenly. Cross-border issues bring on many complexities. Both of these concepts necessitate having protocols to react. In practice, however, the respondents to our survey say they face significant challenges in building and deploying such a process.

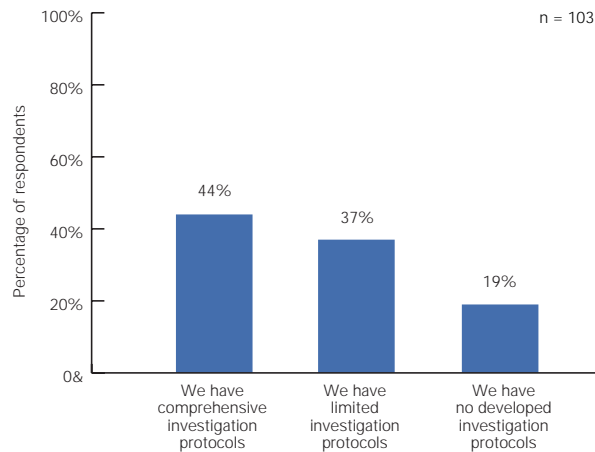
A substantial portion (56 percent) of the investigations professionals interviewed as part of the survey said their companies do not have comprehensive investigation protocols. Thirty-seven percent of respondents said they had "limited investigation protocols," and 19 percent reported not having developed investigation protocols at all. Asia-Pacific-headquartered corporations were least likely to have developed comprehensive protocols.

The 37 percent of respondents who said they had limited protocols also mentioned that their protocols typically deal only with limited aspects of investigations, such as:

- Organizational aspects of assigning resources
- The company's response process to a whistleblower
- Handling evidence.

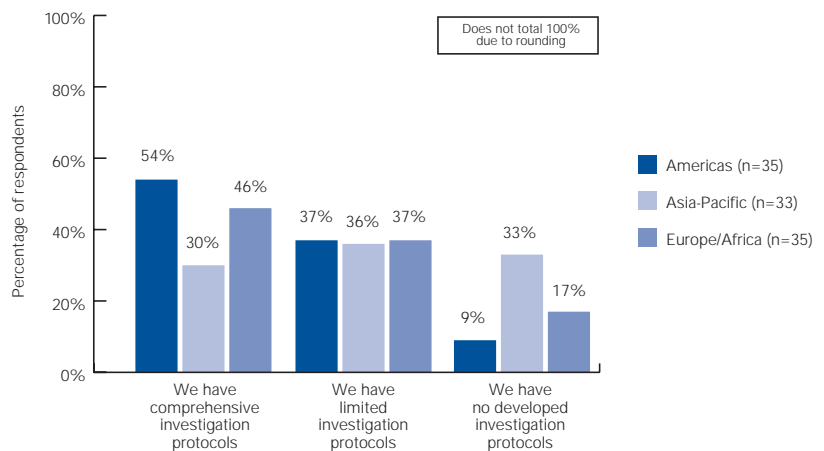
When fraud or misconduct is alleged or discovered, organizations must have assurance that those involved in investigating the incident have and understand the processes needed to identify and scope the issues. We asked respondents to rank elements of an investigation in terms of challenging to very challenging. Identification and scoping of issues was the most common area to be identified as challenging or very challenging.

Less than half of the respondents have comprehensive protocols for conducting an investigation; one in five have no protocols



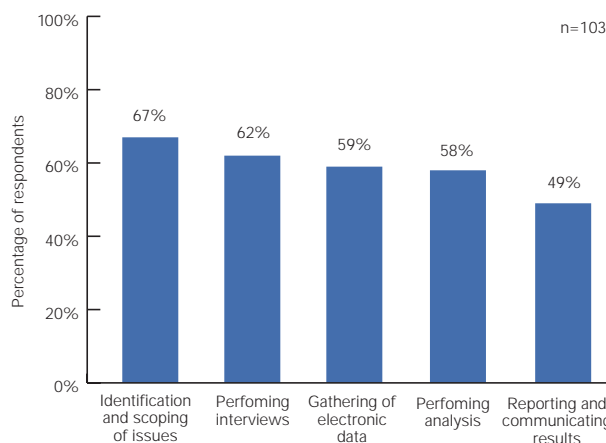
Source: KPMG International, 2007

Extent of investigative protocols by region



Source: KPMG International, 2007

Most significant investigative challenges



Source: KPMG International, 2007

Following are some of the comments from respondents concerning protocols and operating procedures that illustrate the current attitudes and conditions within the survey group. The responses are anonymous in order to protect the identities of the individuals and the organizations:

“We have written protocols in the sense of how to handle evidence, how to handle informants, but not how to conduct an enquiry.”

Chief of corporate security

“We have some [formal protocols] around investigations following reports that are made through our whistleblowing hotline, but those are the only formal guidelines that I’m aware of.”

Vice president of corporate audit

“Is there a protocol? Is there something that [our investigators] can follow? What we find is that unfortunately there’s not...That’s probably one of our biggest issues.”

Vice president, corporate security

“It’s very important [for the organization to have a written, formal procedure/ protocol for cross-border investigations] because the end result of any work we do is an appearance at some formal court or tribunal. That generally doesn’t happen, but we conduct our investigations with the view that one day we will end up at court or a tribunal. We have to do it in a manner that is going to withstand the rigors of a good criminal or civil defense. So we have to comply with the rules of evidence, the rules of natural justice, and industrial relations rule.”

Chief of global investigations

“It is very important because you need to give a consistent message in how you handle and deal with these sorts of things.”

Head of corporate assurance

“The whistleblower program has got a page that says that this is the group that is responsible for doing investigations and this is broadly how they will go about it....It assigns responsibility for conducting the investigation. It doesn’t go into a lot of detail as to each step or stage of the investigation.”

Manager, risk management

Meeting the Challenge of Taking the Appropriate First Steps



Our experience when conducting cross-border investigations, and when discussing such investigations with experienced investigations professionals around the world, has been that businesses face immediate challenges at the initial stage of the investigation.

The level of investigation capability in many organizations is not keeping pace with the geographical operations of the organization or with the sophistication of the fraud and misconduct being perpetrated.

Examples of Dangerous Flaws in the Initial Reaction Stage.

- Taking too narrow an approach in responding to allegations, failing to ensure that sufficient procedures are actually being followed, or taking a view that in some jurisdictions there is little that can be done.
- Failing to properly preserve electronic information – organizations that either must, by regulation, or ought to, for good practice, issue preservation/retention notices should make certain that all relevant parties in all affected geographic locations receive the notice and understand it. We have seen many examples where corporate responses to incidents have not led to prompt preservation/securing of relevant electronic information and many cases where such information was inappropriately accessed causing loss of data and/or damage to the evidence trail.

- Failing to keep the circle tight – the organization should take care in terms of whom to notify or involve during the early stages. If the people who are targets know about or suspect that an investigation is underway, they could destroy vital information or begin to collaborate with others to build a contradictory story.
- Not having the appropriate person to lead the process – in some cases this person could be an independent board member, although not all cases would warrant that level of attention. The point person might also be a security director, the general counsel, or outside legal adviser, depending on the circumstances.

It is all-too common for organizations operating across borders to lack the capabilities to react properly and decisively in response to allegations of improper acts. Organizations also commonly fail to alert the legal department of the matter in a timely manner, and they sometimes incorrectly assume that home-country investigation protocols will apply in all of the geographic locations where the organization operates. Unfortunately, too often, initial reactions tend to be flawed, which can have serious, long-term consequences on the eventual outcome of the investigation. For instance, companies could be subjected to greater penalties and fines by government enforcement agencies regulators should they be found to have handled an investigation poorly.

Possible Considerations for Organizations.

- Undertake an assessment of the business's global investigational capabilities, and benchmark those capabilities against recognized "better practice."
- Assess the organization's investigation competence and adequacy of protocols at the highest levels of the company, and then place the issues on the agenda of the board and audit committee.
- Have a single, global point of accountability for responding to suspicions or actual incidents of fraud and misconduct.
- Prepare investigation resources on the uniqueness of cross-border fraud and misconduct issues and on how to respond to incidents occurring across jurisdictions and cultures. In many cross-border investigations, the in-house investigators do not have experience in managing issues across borders and diverse cultures.
- Consider the development of a written incident-response document. This is not to say there should be a comprehensive handbook on "how to" conduct an investigation, however organizations can benefit from having a comprehensive set of protocols or a procedural manual for responding to a situation that requires investigation. By putting in place clearly defined processes, organizations can develop their responses to an investi-



gation in a reasoned and planned manner, rather than reacting to a crisis situation.

- Begin an evaluation of the organization's information technology environment as it relates to initial steps in obtaining and preserving information that could be used in a cross-border investigation. It is important that the organization has an appreciation of how quickly information can be retrieved from its systems in disparate global locations, and that it has adequate response programs in place.
- Involve legal counsel in any aspect of creating initial protocols and operating procedures, especially those that involve taking actions that could affect the gathering of information or evidence.

Having protocols in place is like having fire drills. In such a drill, everyone knows what they are supposed to do, where they are supposed to go, and to whom they are supposed to report. With protocols, the job of doing the investigation under difficult circumstances may be better managed.

Possible Topics in a Set of Protocols or Procedure Manual.

- Proper assessment of the issue at hand. Develop a case categorization and prioritization model to give a measured response – quickly, but in a planned way – followed by an escalation process in terms of response time, resourcing, and, where relevant, notification to the board and audit committee, depending on the nature of the issue.
 - Planning and managing the investigation – failing to plan is planning to fail. A standard process for planning and managing the investigation helps drive consistency, thoroughness, and good practice, while balancing the need for prompt action.
 - Evidence collection. Standardized evidence collection processes – such as those dealing with witness statements, interview plans, and reports – and a procedure to collect and record physical evidence properly will help avoid questions about contamination of evidence should the matter be taken to court. Also critical are clear guidelines on preservation of electronic and other material and the do's and don'ts of how to handle it.
 - Establish a memorandum of understanding or a service-level agreement with investigations support teams in the locations where the organization operates to facilitate rapid and effective deployment against understood, high-quality response standards.
- Information about the proper way to receive and record the allegation, and how to evaluate the quality of the allegation received.

Cultural and Legal Differences

In a ranking by survey respondents of the top challenges businesses face when conducting a cross-border investigation, four of the top six dealt with culture and local processes. Part of the difficulty stems from the desire by multinational organizations to establish similar policies and operations across the countries where they operate, while at the same time dealing with the many different ways trade is conducted and investigations handled by businesses and local authorities.

"I think one challenge is definitely the different cultures that exist in different countries and trying to get the right balance between expected corporate behavior in Australia, governance and the like, versus what might be acceptable in different countries, be it Indonesia or Iraq or wherever. Whenever there is an allegation in another country you need to be conscious not to simply apply Australian law or Australian culture or Australian behaviors to that country. Often business is done differently."

Head of risk management and internal audit

The challenges cited by survey respondents included those of understanding and operating in the legal or regulatory environment, having an appreciation for cultural differences, language differences, and lack of cooperation from government agencies where the investigation took place. There are also differing legal and evidence procurement requirements. A key consideration in this respect is having an understanding of the standards for maintaining privacy of information and recognizing and protecting confidentiality.

"I think the cultural differences are number one. That challenge actually leads to another set of challenges. It is difficult to work with different cultures in different countries. It is indeed very difficult to work with authorities in different cultures and countries; you have to sort of adopt practices and policies and even codes of conduct and unwritten rules. Cultures really are the most challenging part."

Chief internal audit officer

More broadly, working with foreign governments can be problematic, particularly if the subject of the investigation is a government official or is otherwise connected to the country's business or legal establishment. Many respondents said that because standards for business practices and behavior differ from those of the corporations' country of domicile, they frequently run the risk of serious missteps throughout the investigation. In some cases, the respondents reported that laws are applied unevenly, which makes carrying out an investigation especially difficult without having a working relationship with local officials.

"In a cross-border investigation, I've learned that before I start I must have an understanding of the legal system. That has always helped. There have been instances where we thought our disciplinary codes and practices were applicable and we've found out that, to our horror, they weren't. If I've set up a meeting with partners from different disciplines in a law firm there, I'm going to get a crash course in the law system first."

Forensic audit manager

"It's a straightforward thing where there is a legal environment that must be respected. There are countries where the local authorities are quite happy for you to do the job, but in the case of [name of country withheld] they basically told us which was the playing field we would be acting on and which was the part they would be acting on. This should be respected. In principle, when we have a case where there is an interest from the public side, we really do collaborate in a constructive way."

Head of corporate audit

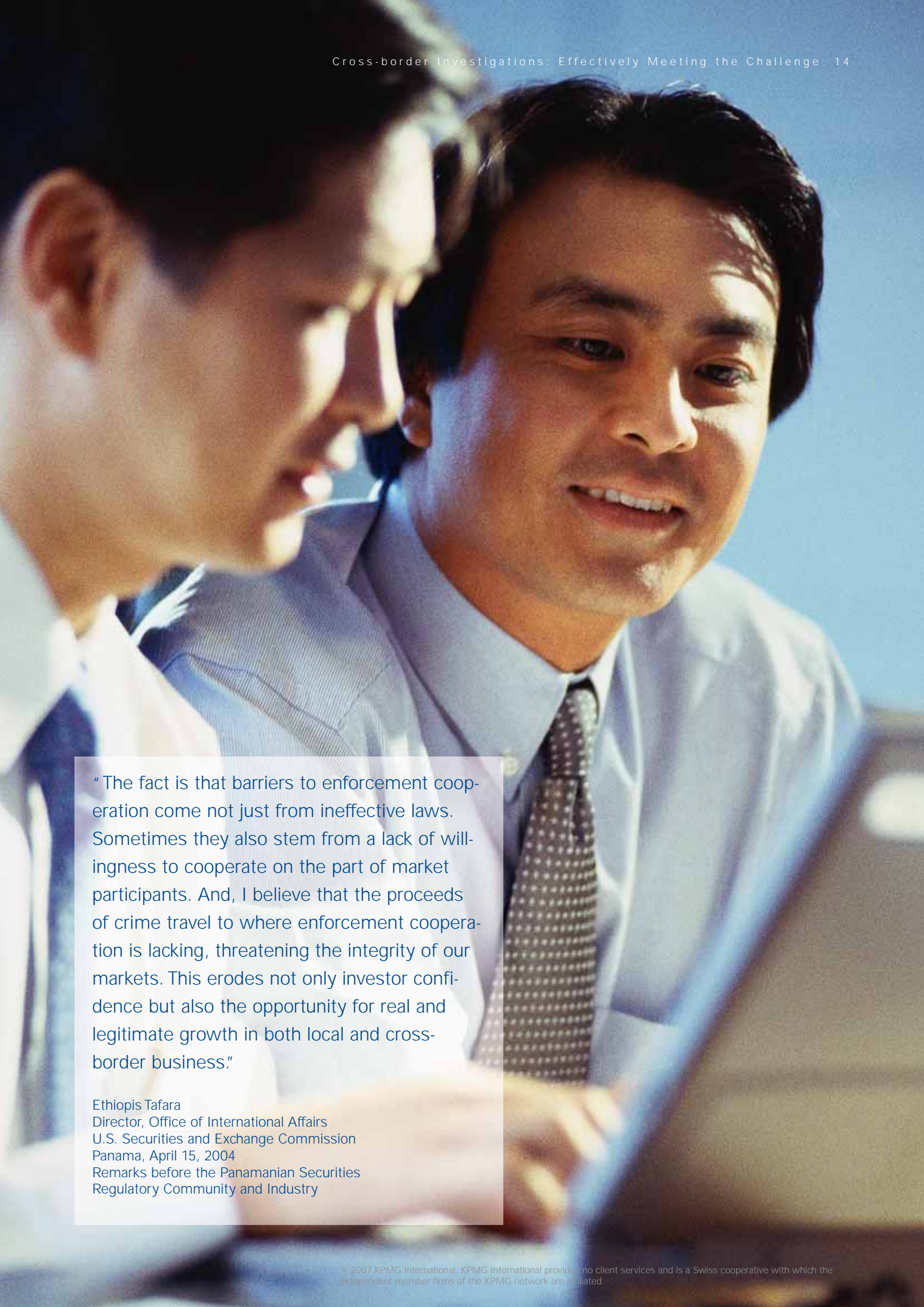
"I can refer to one case I handled where the marketing division was involved. We were in one part of the country and this fraud had taken place in another part of the country. It was just like going to another country and doing an investigation."

Internal audit manager

Senior security executives say the importance of a close working relationship with local officials and law enforcement personnel in countries where an investigation is taking place cannot be overstated. A good relationship with those parties, they say, may make the difference in a good or bad investigation. Many corporate security executives candidly admit that they frequently have difficult issues with local officials in the course of investigations, and simply accept those challenges as a part of doing business.

"It's an inevitable fact of life that the police in [name of country withheld] will, 80 percent of the time, act corruptly."

Corporate security executive

A photograph of two men in business attire, one in a white shirt and blue tie, and the other in a light blue shirt and patterned tie, looking at a laptop screen. The background is a bright, clear blue sky.

“ The fact is that barriers to enforcement cooperation come not just from ineffective laws. Sometimes they also stem from a lack of willingness to cooperate on the part of market participants. And, I believe that the proceeds of crime travel to where enforcement cooperation is lacking, threatening the integrity of our markets. This erodes not only investor confidence but also the opportunity for real and legitimate growth in both local and cross-border business.”

Ethiopsis Tafara
Director, Office of International Affairs
U.S. Securities and Exchange Commission
Panama, April 15, 2004
Remarks before the Panamanian Securities
Regulatory Community and Industry

Meeting the Challenge of Cultural and Legal Differences



A cross-border fraud and misconduct investigation cannot be undertaken from a totally domestic orientation. Simply understanding that key part of the response to a fraud and misconduct investigation can lower the possibility of an immediate obstacle when beginning the probe. In some companies, such a change of orientation may require a significant shift in internal culture.

In every cross-border fraud and misconduct investigation the cultural differences should be taken into account without jeopardizing the internal investigation guidelines. In different cultures different routes can lead to the same outcome. In some cultures the local management should be heavily involved to get the proper cooperation of local staff; in other countries this should be avoided as much as possible. The same is applicable to the involvement of law enforcement. A well-known issue of cultural differences is interviewing. Certain behavior during an interview sometimes is considered a signal of being guilty in one culture and as perfectly normal behavior in another culture.

What follows below are suggestions on how to deal with cultural aspects of a cross-border investigation from the perspectives of language, local customs and traditions, understanding local laws, and working with foreign governments and local authorities.

Language

Language is not a barrier easily overcome. Companies regularly need to balance the requirement to recruit employees in countries of operation who have the relevant skills and experience with the desire to recruit employees with multilingual capabilities. In general, the requirement to have relevant experience and the ability to perform the role in the employing country will take precedence over any desire for multi-language abilities.

When the need arises for a cross-border investigation where language barriers may cause difficulties, a key consideration in selecting team members is to ensure that communications within and with the team are understood. In particular, when interviewing a witness or a suspect, it is important that those to be interviewed are comfortable during the interview and that the investigator has confidence that both the questions and answers are clearly understood. The nuances of answers and how to develop questions can be critically affected by impaired understanding of the question and/or the answer.

Consideration should therefore be given to how best this clear communication can be achieved. This may involve a choice between using a reputable translator to accompany the investigator to assist in the interview process. Often, investigation teams use local specialists from the country in which the investigation is taking place and who have the forensic investigation and specific language skills.

Local Customs

Differences in local customs are a frequent challenge in performing cross-border investigations. Dealing with this challenge can require an intimate knowledge of country/regional differences and the “do’s and don’ts” in order to avoid hampering the progress of the investigation. Seth T. Taube, a partner and chief of the trial section of the New York office of the international law firm Baker Botts LLP said in a recent interview with KPMG, “It is a necessary fact of life in emerging economies, or economies that up until just a few years ago were closed economies, [that] you have to deal with government officials. In fact, it would be imprudent to conduct business without those relationships.” Taube warned businesses that enter new markets not to try to expect traditional Western business conduct to be followed. “Don’t expect the values we place on contract and such things to be considered values in other cultures, but be ready to control the risks that arise because of this natural tension.”

Executives who have long experience in doing business in other cultures are aware of other themes that require consideration. Their impact on cross-border investigations can be considerable. Such themes include:

- **Maintaining “face.”** This is a very important issue in many cultures, and there is a need to handle this matter delicately. *Face* is a term that is linked with the opposing concepts of honor and humiliation. Therefore, a person who is part of a cross-



border investigation could maintain or lose face, depending on how a question is posed and structured.

- **Demonstrating respect.** Regardless of the circumstances, the utmost respect is required when a cross-border investigation is being conducted. Respect can be affected by body language as well as by the spoken word. Ignorance or nonobservance of certain customs, forms of greeting, and the like may hamper progress. For example, not knowing how to give and receive a business card in Japan or China could lead to offense being taken and a lack of cooperation. Respect also follows seniority, where people in some cultures will do something as directed by a senior, regardless of what they think.
- **Understanding questions and answers.** A person attempting to answer a question in a language that is not his or her native language may not be aware of nuances that could give offense. That situation could present problems if the subject agrees with the interrogator, but hasn't actually fully understood the question. Problems might be overcome by follow-up, written communications after a meeting, or of course by using native-speaking specialist investigators.

Overall, having a "local" on your team is invaluable.

Understanding Local Laws

Local laws and guidance may be quite different from those where the headquarters of a business is located. In order to avoid problems with such matters, it is important for companies with overseas operations to ensure that those likely to be involved in performing investigations are made aware of any relevant local customs and laws. It is also important that they receive adequate training to fully understand these differences and respond appropriately should the need arise to perform a cross-border investigation. If such knowledge is not accumulated and kept up to date in-house, it is even more important to bring into the investigation team appropriately experienced and skilled resources.

Areas of difference may include:

- The attitude of local authorities to "overseas" controlled businesses operating in their country
- What is illegal in one country may be custom and practice in another
- The extent to which the local authorities will expect, require, or pursue prosecution
- How evidence that has been gathered may be used in court
- The evidence required to secure a successful civil outcome or criminal prosecution
- Data privacy legislation.

Working with Governments, Local Officials, and Law Enforcement

This can be a particularly difficult area for many companies and, if not approached correctly, can lead to significant problems, particularly where local governments have the power to influence any ongoing trade of the company.

The payment of bribes is one area that falls under this category and is often a cause of concern for many companies.

In some countries it may be considered normal to pay a "fee" to conduct business, whereas in others such an act is considered to be illegal and may have serious consequences. In particular, this is an issue for consideration by U.S. multinationals, which are required to comply with the U.S. Foreign Corrupt Practices Act in every country in which they operate.

Companies should ensure that they fully understand relevant international and in-country legislation relating to fraud, corruption, and financial misconduct in order to avoid committing any offense in relation to such matters. Such understanding should be obtained and updated by companies on an ongoing basis to ensure that sufficient information is available at the outset of any investigation that may arise.

As mentioned previously, understanding the legal systems in each country and having access on a continuous basis to resources that can assist in such matters is particularly important. It is important when conducting an investigation to know at the outset whether or not it is a requirement to involve law enforcement in that particular country. It is equally important to know if and when civil or criminal action can be initiated and what the process for this would be.

If the correct steps are not taken throughout the investigation, difficulties could result going forward.

Resources

Organizations will differ when it comes to which resources to utilize in a cross-border investigation. As a potential need for an investigation arises, the selection of the resources will be influenced by past experiences, the capabilities of its personnel, and its knowledge of what external resources are available. However, thoughtful and deliberate planning that addresses the preparedness of your internal capabilities and becoming familiar with external resources are advisable.

"We had a dedicated investigations function for [issues] that are raised through our whistleblower program, but for any investigations that are generated or required outside of that whistleblower program, there is no dedicated group or person that must be the investigator."

Manager, internal audit and risk management

"In a cross-border investigation... there have been instances where we thought our disciplinary codes and practices were applicable and we've found out that, to our horror, they weren't....When we want to analyze data, we very often outsource that. We have found we've got good value doing that. It's very time-consuming and we don't have the resources to do it."

Group forensic audit manager

Even in companies that reported having a dedicated cross-border investigation function, survey participants said investigations responsibilities were typically shared with other functions, including human resources, legal, and internal audit.

"I have the resources of the internal audit department at my disposal as well as members of human resources at my disposal, depending on the situation. For example, I may commit members of the internal audit department to assist in conducting a financial, what I call forensic review. Additionally, I have members of a security IT group that have a dotted line to me that I engage to assist in conducting the IT portion of investigations."

Vice president, information and security

Internal audit was cited very frequently as the function that owned or shared the cross-border investigations function:

"Internal audit, together with the business security [department], is responsible for conducting investigations about frauds in the company... All the [investigation] procedures adopted were based on internal audit procedures."

I am an internal auditor, or the manager of internal audit. All the investigations are within my role. In other words, I am in charge of all investigations."

Head of internal audit

Across geographies, respondents who reported struggling with resource issues said the most pressing challenge they faced is that associated with having people with the requisite depth and breadth of investigations skills. Additionally, there was the challenge to assemble and mobilize a team of individuals who would be involved in a cross-border investigation.

"Resources are the biggest issue. I'm going to be blunt – that's our largest challenge."

Vice president corporate security



"Administratively there are probably not enough of us so that when we have an investigation it impacts on the rest of our workload."

Internal audit manager

"It is very difficult to get information extracted from the people in the company because many have changed jobs, and we've got a very poor process of information documents management. We can't easily recover contracts and invoices..."

General auditor

Some respondents said they are also hindered by a lack of specific investigation processes and protocols for dealing with other company functions and departments. Further, they reported needing assistance in dealing with local personnel involved in the investigation, for putting together and mobilizing investigation teams, and understanding the legal issues in the countries in which they operate.

Those who said they believed the cross-border investigation worked well cited the importance of good relationships with the groups that shared the duties.

"There are totally open communication lines between the audit teams as well as the legal functions."

Head of corporate assurance



“When you have an in-house component, you get this aggregated knowledge of how the operation runs. It’s very, very useful...You can’t do it all, and there is a need to cohabit with your consultants out there. There is a need to use them expeditiously and widely.”

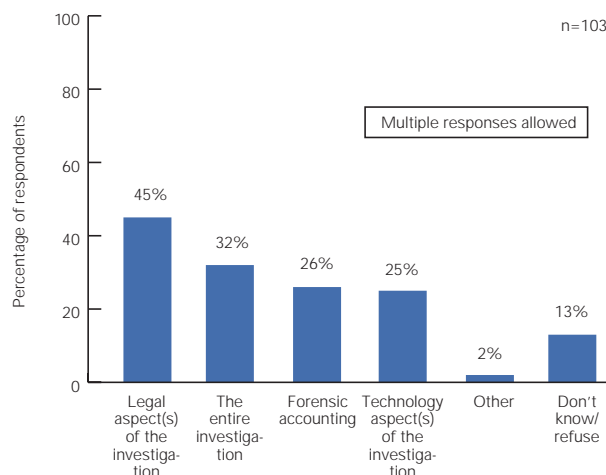
Group forensic audit manager

Not surprisingly, the difficulties surrounding having enough – and the proper – resources lead organizations to look for outside help when conducting cross-border investigations. Participants said the primary reason for going outside their organizations to fill resource gaps is because they do not carry dedicated specialists on their staff since the need is periodic rather than recurrent. Nearly one third (32 percent) of participants said they used external resources for the entire investigation, and almost half (45 percent) said they engaged an outside law firm to handle the legal aspects.

Additionally, they believe that use of outside specialists:

- Would bring forth the perception of having an independent organization to lead an investigation
- Could provide speed and responsiveness when an incident occurs
- Could help protect the integrity of information gained during the investigation

Nearly half of the respondents say external resources assisted with legal aspect(s); one in three say such resources helped with the entire investigation



Source: KPMG International, 2007

- Would be useful for computer forensics support
- Would be useful for surveillance support.

“ [Having the right internal resources] is an issue for two reasons. One, we are not a big enough company to have a dedicated investigation unit. It’s sort of a subset of what we can do....And expertise-wise, we are not as strong because we are not big enough to have dedicated experts with the right background for conducting investigations, hence the need to use [outside] experts.”

Chief of internal audit

“ Because this was such a high-profile issue and it was in the newspapers, we really needed to provide to both the directors and external agencies more assurance it was being dealt with at an arm’s-length and at a professional level. Hence, we engaged [outside experts] to assist.”

Chief of audit

“ We outsourced it. We don’t want to be accused of manipulating anything.”

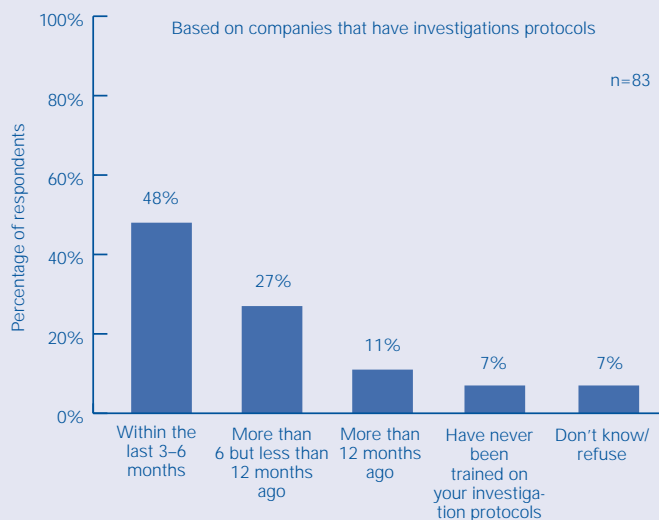
Group forensic audit manager

Meeting the Challenge of Resources



When an organization faces the need for a cross-border investigation there are almost always tradeoffs when it comes to resources.

Half of respondents say their staff has not been trained on investigation protocols within the last six months



Source: KPMG International, 2007

Education on current trends and formulating responses to those trends is vital for the cross-border investigation function at multinational organizations. The global marketplace continues to change quickly, as national borders become less of an obstacle to trade around the world. That change has added an entirely new dimension for multinational organizations that must react quickly and effectively as fraud and misconduct occurs. Ongoing training among members of an organization's incident response team may mean the difference between effectively handling an incident and making a bad decision at the start of an investigation.

Effective cross-border investigation teams or individuals should have a broad understanding of the company's business strategy and have a background in business processes and finance. The top managers should consciously build an internal investigations team with a capability of handling routine investigations in the organization. And, like a typical internal arrangement with a third party, the managers should also consider having a close alliance with an external organization that can provide specialized and effective support when cross-border fraud or misconduct occurs. Recognizing that it probably is cost-prohibitive to have

highly qualified investigators on staff in every offshore location where the business has offices, an alliance with an organization that can provide a combination of data analysis skills, forensic technology capabilities, and a solid understanding of the language and business processes in those locations would provide an advantage should the need for a cross-border investigation arise.

Considerations for a board of directors or management when assigning or identifying resources for a cross-border investigation:

- **Skill set.** Assess the nature of the incident, suspicion, or allegation, and then assess the organization's skills to handle the matter. The purpose of this step is to determine the combination of legal, forensic accounting, technology, and industry expertise that is required to handle the matter. Bear in mind that in certain jurisdictions it may be customary for a legal team to be initially engaged. The legal team may want to hire other resources for the purpose of establishing legal privilege. Issues that have financial or accounting consequences almost certainly will require forensic accountants. Where electronic evidence exists, such as e-mail, it will be necessary to have forensic technology resources as part of the team. Industry expertise can especially be useful in engagements at organizations within regulated industries, such as banking,



insurance, energy, healthcare and pharmaceuticals.

- **Capabilities**

- *Experience.* Investigations are always sensitive matters. Therefore it is imperative that the investigation team has the background and experience to meet the challenge. If the organization has its own team or if it decides to hire a third party, senior management – or the board – should determine if the team has “been there before,” and how it has handled difficult situations. Management or the board may want to be wary of an investigator who claims to have seen an exact situation before, or predicts the ultimate outcome. Investigations rarely play out as expected. An investigator should be able to describe a general preliminary approach to the matter, but should not present an inflexible work plan.
- *Technical expertise.* Meet with prospective investigators to gain an understanding of both the preliminary approach the investigation team proposes and the expertise of the team’s key members. If possible use experienced investigators to perform the interviews. If the investigation will involve the gathering, storage, or transportation of electronic evidence, organizations should explore the background of those performing the preservation of the data and how they will go about those activities.

- *Background and credentials.* Many investigators develop skills in the public sector as government agents or by virtue of a legal or regulatory background. Forensic accounting has emerged over the past two decades as a specialized profession. It can take five to ten years of working on investigations before a forensic accounting specialist can grasp the complexities and develop the professional maturity necessary to manage investigations. There are some formal credentials that have also started to emerge as being recognized within the field of forensic accounting, such as the certified fraud examiner.

- **Independence.** In many instances, the ability to demonstrate the independence of the investigation is imperative. For example, an organization would not want its general counsel investigating the chief executive officer, nor would it want internal audit investigating the chief financial officer. The more independent the resources, the more easily stakeholders of investigations (such as regulators, investors, and external auditors) will accept the findings of an investigation.
- **Availability.** Investigations nearly always require immediate attention and the investigation resources have to be able to assemble a qualified team quickly. A fast response is more difficult in cross-border situations. While some organizations will have direct resources in foreign locations that can be deployed, it would be a mistake to assume that all large businesses would have these resources and have the ability to act quickly. Senior management or boards should determine whether the investigative resources in the disparate locations have similar investigative backgrounds, or if they hire local “bodies” that do not have the same training and experience.

As mentioned above in the discussion dealing with initial protocol and operational procedures, a single, global point of accountability is a critical capability for any multinational organization operating in an environment where rapid communications can facilitate fast-spreading illegal or improper activities. In its discussion of resources, senior management or the board must have comfort concerning its ability to respond in a number of jurisdictions, each with disparate cultural approaches to law enforcement. Without that capability, a company may find that it is vulnerable to a number of negative consequences.

The Availability and Accessibility of Electronic Data



One of the commonly cited challenges among survey respondents was not knowing where to find data that is relevant to a cross-border investigation. When asked to rank factors that had an impact on conducting cross-border investigations, a third of respondents cited the availability and accessibility of electronic data. Cross-border investigations pose unique challenges relating to locating data, particularly when such directives as retention policies do not exist or are not followed, as some of the survey respondents reported.

One reason for the difficulty may be the proliferation of portable storage devices, such as USB flash drives or “thumb-drives,” cellular telephones with removable memory chips, or personal digital assistants (PDAs). At times, data that is relevant to a cross-border investigation may be on the personal computer (PC) of an individual who has left the company for another job and not returned the PC. In still other cases, a PC may have been taken out of service and not stored according to company policy, and thus the information cannot be retrieved.

Another common instance is where a company PC or laptop used by an exiting employee is reallocated to another employee, sometimes after being “cleaned down” by the company in some way, thus making retrieval of usable evidence more difficult. Further, some respondents said that although they knew where the data resided, they weren’t clear on the rules and regulations relating to access and transportation of data.

The issue of physical access to relevant data is a particularly vexing one for many companies with business units spread around the globe. A business that is headquartered in Berlin, for example, may not be able to immediately take physical possession of data that is on a PC located in, say, Ho Chi Minh City, simply because of the need to discreetly travel to the Socialist Republic of Vietnam. The company may be able to use the company's network to view and possibly acquire the data, but be unable to quickly and quietly travel to the far-off location.

Aside from the physical limitations of data collection, many countries, particularly in Europe, have data privacy laws that place restrictions on how data can be collected and how it can be transported – if at all. Many countries require that explicit consent agreements be reached between the business and the affected individual.

“Privacy of information is our biggest problem. And a number of different countries around the world have their own particular areas where it's difficult to get certain information.”

Manager, investigation function

“Between Europe and North America, the privacy laws are much more stringent. For instance my counterpart who's located in Stuttgart cannot just go in and access someone's work network, their e-mail account or their hard drive. In the United States, in Canada or Mexico, within our policies, that is company property from two respects. Number one we own the hardware and the software, and all the storage devices that are used, so therefore that gives us legal access. Plus when things are inputted into that system, it is done by employees who we are paying for that time and we have policies that require that be work related kind of

information. Plus whenever you turn on your computer, it tells you that anything done on a computer is considered property of the company and that we have the right to inspect, seize, take control at any time we wish. It's generally been upheld in the court, it's not a problem in Mexico, it's not a problem in Canada. It is a problem in Europe.”

Manager, security services

The challenges associated with the availability and accessibility of data involve a number of interrelated issues. Aside from their struggle to stay current on the disparate laws and regulations around the world dealing with data collection, storage, and transport, respondents cited problems with inconsistencies in their companies' procedures regarding data collection from one location to the next. In addition, there is the challenge of the sometimes unrealistic expectations placed on in-house investigators to effectively launch and carry out data gathering in all of the countries where the fraud or misconduct might have occurred.

Organizations that recently established business units in a number of new locations due to global expansion or having entered into mergers, joint ventures, or strategic alliances have seen their problem of accessing data exacerbated. Many may also have systems-integration issues that have not been resolved as a result of expansion or alliances.

We noted with interest that 75 percent of respondents said they believe they have adequate technology resources to support investigations. This is inconsistent with our experience in investigations where we see that a substantial proportion of companies do not have the specialist technology software and operational procedures that should be deployed when seeking to capture and

analyze electronic data in an effective, secure, and evidentially usable manner. The statistics in the survey could therefore be interpreted as indicating a gap between companies' perceptions as to their investigative IT capabilities and what may be the reality compared with good investigative practice.

The majority of survey respondents (69 percent) said IT proficiency is important to the success of cross-border investigations. Interestingly, respondents who reported having comprehensive investigation protocols rate the importance of IT proficiency higher (82 percent) than those respondents who said they did not have comprehensive protocols (59 percent).

It would be difficult to argue against the idea that the efficient deployment of technology coupled with effectively using the capabilities of those who work with the technology can make or break a cross-border fraud and misconduct investigation. Our experience and in-depth discussions with survey respondents indicate that the kind of technology employed by perpetrators of fraud is sometimes a generation ahead of the technology of the victim. The nature of fraud, after all, is to discover and exploit weakness in the security of valuable assets. Fraud surveys of business executives conducted in 2006 by KPMG member firms in Australia, New Zealand, and India revealed that fraud and misconduct is likely to increase in the years ahead. In virtually every interview conducted as part of this project, survey respondents reported that internal control weaknesses were exploited in the commission of the crimes against their organizations.

An Asia-based executive dealing with a cross-border fraud described the role of technology in a recent incident in the following way:

“Criminals just become creative in the way of doing things. I suppose continued advancement in the area of IT has made it so much simpler for the crooks to defraud us. We’ve got false websites allegedly operating in Australia which are being run out of the U.S. or Europe.”

Getting better at using technology capabilities clearly is on the agenda of businesses around the world. Almost 80 percent of respondents say they believe in the next five years IT proficiency will be even more important than it is now to the success of cross-border investigations.

“I think it depends on the company. Within our company, our systems aren’t that fantastic. To use data-mining tools and things isn’t always very easy nor appropriate. But I’m sure in other companies with, perhaps, more sophistication from an IT point of view, those things can be fantastic in terms of identifying transactions that are inappropriate or outside the norm.”

Former head of ethics and internal audit

Safe Harbor Regulations and Cross-Border Investigations

One area of legislation that impacts how companies can access electronic data in international fraud investigations relates to the European Union’s Directive on Data Protection (95/46/EC). This directive, which went into effect in October 1998, would, and prohibits the transfer of personal data to non-EU nations that do not meet the European “adequacy” standard for privacy protection. While the United States and the EU share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the EU, relying on a mix of legislation, regulation, and self-regulation, while the EU requires creation of government data protection agencies, registration of data bases with those agencies, and in some instances prior approval before personal data processing may begin. As a result of these different privacy approaches, the directive could have significantly hampered the ability of U.S. companies to engage in many international cross-border transactions, including investigations.

As part of the Data Protection Directive, the United States and the EU entered into the so-called “Safe Harbor Agreement,” designed to bridge different privacy approaches between the EU and the United States and offer a streamlined means for U.S. organizations to comply with the Data Protection Directive. Under this agreement, data transfers from the EU can take place to U.S. companies that agree to meet certain intermediate privacy protection standards. The financial services industry, however, is excluded from the Safe Harbor Agreement because of recent changes in U.S. financial privacy laws under the Gramm-Leach-Bliley Act (GLBA). In the United States, private-sector adoption of the agreement was slow to start.

Although the non-transferability provisions of the Data Protection Directive have yet to be rigorously enforced, financial institutions that currently have no acceptable Safe Harbor alternatives that guarantee the transferability of personal data for the long term will be unable to secure the uninterrupted ability to transfer data from the EU to the United States. Negotiations over the Safe Harbor Agreement, however, continue to evolve. For example, while the financial services sector was not included in the Safe Harbor Agreement originally, now that GLBA is being implemented, both sides are revisiting issues related to financial privacy.



Meeting the Challenge of Availability and Accessibility of Electronic Data



Obtaining electronic data is critical to the success of a cross-border investigation, but the rules to get access to data sometimes can be complex. That is why it is imperative that there is an adequate understanding of the rules and regulations regarding gathering, transporting, and storing data.

Following are recommendations about access to electronic data that organizations may consider in the context of cross-border investigations:

- Approach all cross-border investigations from the perspective of preserving the integrity of the data. The mere suspicion that an organization has destroyed, tampered with, or attempted to hide data from regulators or prosecutors could seriously harm the reputation of a company. Having a documented set of protocols that has been clearly implemented consistently across an organization gives credibility to the results of an investigation.
- Review the organization's procedures for the issuance and enforcement of a preservation notice, that tells individuals that the company is under an obligation to preserve all information relating to a particular instance because the company is being sued, suspects that fraud or misconduct has occurred, or is under investigation.

Organizations may want to consider asking the following questions:

- What are the company's retention policies, including in relation to e-mails?
- What is your data back-up retention policy?
- Where do you allow people to store data on your servers?
- How much information do people replicate on their hard drives?
- Where are the servers on which relevant data is stored, and are they all under the company's control?
- Review the company's protocols regarding the rotation of back-up data tapes. There should be a process in place that ensures that the rotation schedule will not allow critical data to be written over once a preservation order is implemented.
- Organizations should institute training programs on their electronically stored information policies and procedures. There should be information on data privacy laws and forensic preservation in the organization's incident-response plan, along with the requirement that all affected individuals take responsibility for familiarizing themselves with the information.

- Individuals who have a role in cross-border investigations need to have a deep understanding of the laws on the gathering, storage, and transportation of evidence across international borders. While senior management cannot be expected to have an in-depth understanding of the rules, it is important for the organization to gain an appreciation for the variability of such rules and laws in order to avoid costly mistakes when an investigation is launched.
- The individual with the responsibility for being the global point of accountability to respond to allegations should make certain that the business has access to country-by-country details on procedures and requirements for gathering, storing, and transporting data. Individual country laws continue to evolve, and organizations must always be alert to any recent changes in such laws and seek to understand them.
- When a company seeks help from an outside organization to investigate cross-border fraud and misconduct, it must be assured that the third party also has a detailed, up-to-date knowledge of the rules and best practice for collection, preservation, and transmittal of data in and across the relevant jurisdictional boundaries. This can raise challenges in any or all

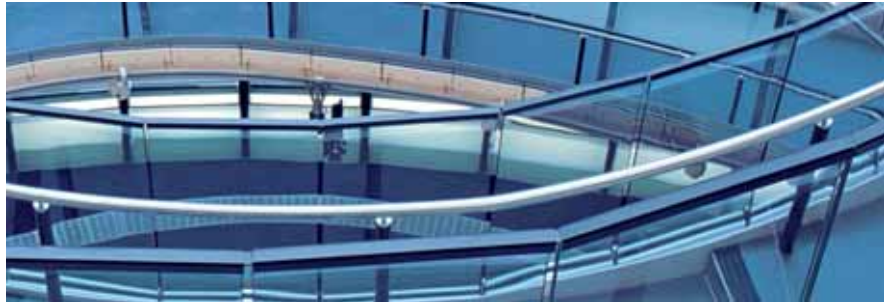


data capture, in-country review, transmittal across jurisdictional boundaries, and review out of country – for instance, at the group’s head office or legal advisers’ offices. Using an organization that has numerous and unconnected teams heightens the probability of damaging the integrity of the investigation. Companies can help avoid significant problems during the course of the investigation as well as possible difficulties in subsequent criminal prosecution or civil litigation by having a focused work plan that has been verified by appropriately experienced forensic IT professionals and a process that clarifies the chain of custody of evidence while protecting the integrity of the data.

- Organizations should ensure that when a cross-border investigation is launched they have the ability to track the evidence that is being gathered in all locations around the globe, and that the method employed to gather the information is uniform.



Key Points to Remember



The challenges associated with conducting cross-border investigations are complex, lending weight to the imperative for being properly prepared when incidents of fraud, corruption, and misconduct occur. An appropriate initial response can have a profoundly positive impact on the outcome. Wise organizations think first, and then act.

At the same time, no organization can possibly have a total understanding of all the cultural differences or have the laws in each of the locations where it conducts business. Further, an organization doesn't need to know everything. Instead it needs to know where to find what it needs and who to ask.

Frequently, it is the mishandling of electronic data and other evidence that causes problems in a cross-border investigation, given the myriad laws regarding the gathering, transporting, and storage of such data.

An organization should not become comfortable that it knows everything it needs to about cross-border investigations. The landscape changes by the day, which will continue to give rise to new threats, often in different parts of the work. Being ready to respond and flexible in approach will best prepare organizations to react to meet their challenges in cross-border investigations.

Key Contacts

Europe, Middle East and Africa

Richard Powell

Partner

KPMG LLP in the United Kingdom

richardfa.powell@kpmg.co.uk

+44 (0) 161 838 4044

Americas

Phil Ostwalt

Partner

KPMG LLP in the United States

postwalt@kpmg.com

+1 404 222 3327

Asia Pacific

Mark Leishman

Executive Director - Forensic Services

KPMG in South Korea

mleishman1@kr.kpmg.com

+82 (2) 2112 0882

KPMG contributors to this publication include: Phil Ostwalt, Mark Leishman, Richard Powell, Rens Rozekrans, Stephan Drolet, Ken Milliken, Earl Fagan, Amanda Rigby, Jilane V. Khakhar, Timothy R. Dougherty, Anne Hollyday, Lynda Leavitt, Charles Garbowski, and Marshall Bain.

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.

KPMG and the KPMG logo are trademarks of KPMG International, a Swiss cooperative.

© 2007 KPMG International. KPMG International is a Swiss cooperative. 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.

Document code: GSC037