

# Global Fraud Report

---

## Economist Intelligence Unit Survey Results

Theft of information and electronic data surpassing all other frauds

Fear of fraud dissuading companies from going global

Lack of preparation for greater regulatory enforcement

Fraud is predominantly an inside job



## **About the research**

The annual Global Fraud Survey, commissioned by Kroll and carried out by the Economist Intelligence Unit, polled more than 800 senior executives worldwide from a broad range of industries and functions in July and August 2010. Where Economist Intelligence Unit analysis has been quoted in this report, it has been headlined as such. Kroll also undertook its own analysis of the results. As in previous years, these represented a wide range of industries, including notable participation from Financial Services; and Professional Services; as well as Retail and Wholesale; Technology, Media and Telecoms; Healthcare and Pharmaceuticals; Travel, Leisure, and Transportation; Consumer Goods; Construction, Engineering, and Infrastructure; Natural Resources; and Manufacturing. Respondents were senior, with 47% at C-suite level. Fifty one percent of participants came from companies with annual revenues of over \$500 million. Respondents this year included 29% from North America, 25% from Europe, and 24% from the Asia-Pacific region (of whom 47% – more than in previous years – were from China and India); and 11% each from Latin America and the Middle East & Africa.

This report brings together these survey results with the experience and expertise of Kroll and a selection of its affiliates. It includes content written by the Economist Intelligence Unit and other third parties. Kroll would like to thank the Economist Intelligence Unit, Dr. Paul Kielstra and all the authors for their contributions in producing this report.

Values throughout the report are US dollars.

# Global Fraud Report

<b>INTRODUCTION</b>	
Tim Whipple, President, Kroll Consulting .....	4
<b>ECONOMIST INTELLIGENCE UNIT OVERVIEW</b>	
Survey results .....	5
<b>FRAUD AT A GLANCE</b>	
A geographical snapshot .....	8
The regulatory challenges of crossing new frontiers .....	10
<b>MARKET ENTRY</b>	
Facing the fraud challenges of emerging market entry .....	12
Preventing fraud in new acquisitions .....	14
<b>REGIONAL ANALYSIS: AMERICAS</b>	
North America overview .....	16
Data Breach Management: What every company should know .....	17
The SEC cracks down harder on pay to play .....	19
Latin America overview .....	20
Transportation infrastructure fraud in Brazil: Steering clear of the potholes .....	21
Brazil overview .....	23
Battling corruption and fraud in Colombia .....	24
Colombia overview .....	25
Risk governance for mines in emerging markets: The power bottleneck .....	26
<b>REGIONAL ANALYSIS: ASIA-PACIFIC</b>	
Asia-Pacific overview .....	28
Fraud in India's manufacturing and engineering sector .....	29
China overview .....	31
Hand-in-hand: Corruption and private-sector fraud in China .....	32
Preventing the loss of trade secrets in China .....	34
Southeast Asia overview .....	36
Indonesia's darker side .....	37
<b>REGIONAL ANALYSIS: EMEA</b>	
Europe overview .....	38
Investigations and the use of technology .....	39
Fraud in the Gulf: For better or for worse? .....	40
Middle East overview .....	41
Africa overview .....	42
Risk and reward: Fraud and the African telecoms industry .....	42
Lower rates of fraud keep sector on track .....	44
<b>SECTOR SUMMARY</b>	
Summary of sector fraud profiles .....	45
<b>CONTACTS</b>	
Key regional contacts at Kroll .....	47
<b>ECONOMIST INTELLIGENCE UNIT INDUSTRY ANALYSIS</b>	
<b>RETAIL, WHOLESALE &amp; DISTRIBUTION</b> .....	15
<b>HEALTHCARE, PHARMACEUTICALS &amp; BIOTECHNOLOGY</b> .....	18
<b>FINANCIAL SERVICES</b> .....	19
<b>CONSTRUCTION, ENGINEERING &amp; INFRASTRUCTURE</b> .....	22
<b>NATURAL RESOURCES</b> .....	27
<b>MANUFACTURING</b> .....	30
<b>CONSUMER GOODS</b> .....	33
<b>PROFESSIONAL SERVICES</b> .....	39
<b>TECHNOLOGY, MEDIA &amp; TELECOMS</b> .....	43
<b>TRAVEL, LEISURE &amp; TRANSPORTATION</b> .....	44

# Introduction



Welcome to Kroll's fourth annual Global Fraud Report. Our objective remains the same: to raise awareness of emerging trends, in order to help you grow your business securely while minimizing both the likelihood of fraud and scale of its impact.

In this edition, we take a closer look at the issues that Kroll is most frequently asked to investigate, and the variations in the nature of the threat across different regions. Four important themes emerge:

- Theft of information and electronic data overtakes physical theft for the first time as the most frequently reported fraud.
- Fear of fraud is dissuading 48% of companies from operating in other countries. China and Africa are the geographies most affected, with corruption identified as the greatest concern.
- Companies appear unprepared for heightened Foreign Corrupt Practices Act (FCPA) enforcement and the impact of the UK Bribery Act. For example, only one-third of respondents with a presence in the United States or United Kingdom felt the laws applied to them.
- Fraud is largely an inside job across all geographies and industries. Some 44% of respondents attributed fraud to employees and a further 11% identified agents or intermediaries as the key perpetrators.

This year we analyze for the first time fraud losses as a percentage of income. There is cause for concern: fraudsters' take from business increased 20% in the last 12 months. Almost 90% of respondents report being victims of fraud – similar to last year's survey results.

From an industry perspective, we see encouraging declines in fraud prevalence in three sectors: Construction, Retail and Travel. The other seven sectors show an increase, with considerable jumps in Consumer Goods and Technology, Media and Telecoms.

You'll notice that our report looks different this year, reflecting our transition to the Altegrity family of businesses. Altegrity is a portfolio company of Providence Equity Partners, one of the world's premiere private equity firms, with over \$22 billion of equity capital under management. Our acquisition by Altegrity reflects a strong belief in Kroll's proven performance and growth potential in the rapidly growing global market for investigative, compliance and risk management services.

I hope that you find our report enlightening, and that it helps you to identify emerging threats and opportunities for your own business.

Best regards,

**Tim Whipple**  
President, Kroll Consulting

# Economist Intelligence Unit Overview



## Fighting increasing threats

**This year's annual Global Fraud Survey, commissioned by Kroll and carried out by the Economist Intelligence Unit, polled more than 800 senior executives worldwide from a broad range of industries and functions in July and August 2010.**

### **If fraud were a virus, almost everyone would be slightly ill**

Of the respondents, 88% report that they had been hit by at least one type of fraud in the past year, a figure broadly similar in every region and consistent with those of previous years. Record-setting, headline-grabbing scams, such as the Madoff or Satyam frauds, can give a false impression of fraud's financial impact on business. The most successful pathogens do not kill the host, but live off them. Of course, huge, company-destroying losses do occur, but they are very rare. More typical are smaller losses over months or years.

In isolation, this appears to be good news. The frequent repetition of small losses, however, can create a significant problem in aggregate. In the past, this report has presented the figures for an average overall fraud loss, but such a figure is less instructive than it might seem: levels of loss are closely associated with the size of companies. Instead, it is more meaningful to report losses as a proportion of income. By this measure, the take of fraudsters from business rose by more than 20% in the last 12 months, from \$1.4 million per billion dollars of sales to \$1.7 million.

Fraud, then, is only rarely an acute disease threatening the whole body. It is frequently, however, a widespread virus that, while usually draining limited resources from the host, is always ready to flare up when the opportunity arises. And like a virus, fraud is constantly mutating, and can, if left unchecked, become life-threatening. This year's Global Fraud Survey digs deeper than previous years to offer an insight into the sources and impact of fraud and the perceptions of senior business executives around the world. The findings highlight several key trends:

### **Theft of information and electronic data surpass all other frauds for the first time**

Information theft has become the most common form of fraud. In previous Global Fraud Surveys, the theft of physical assets or stock has always been the most widespread fraud by a considerable margin. In 2009, for example, 28% of companies surveyed reported suffering physical theft, while the next most common fraud – management conflict of interest – affected only 20%. This year, however, as Chart 1 (overleaf) shows, information theft, loss or attack has become, by a small margin, the most commonly reported fraud. It is not that fraudsters are switching away from other methods: the increases and decreases in other categories are of the sort that could be expected in this type of survey. Rather, information theft grew significantly.

Such growth is never uniform across the economy. As Chart 2 indicates, information-rich industries such as Financial Services, Professional Services, and Technology, Media and Telecoms itself are the most likely to be hit. The chart also indicates, however, that the problem is far from isolated.

The survey suggests that things may get worse before they get better. Information theft or attack is the type of fraud to which respondents are most likely to describe their companies as vulnerable (37%). Again, their concerns are not isolated. This type of crime is regarded as the greatest weak spot for three of the 10 industries covered in the survey – Financial Services, Professional Services, and Natural Resources – and the second-greatest for three more – Construction, Technology, Media and Telecoms, and Retail.

### **Corporate information technology systems are increasingly under threat**

Criminals have always targeted physical assets because they are present in almost all companies, are frequently simple to steal, and have a tangible value which makes them easy to convert to financial gain. The increasing prevalence of information technology has made the same attributes increasingly true of data. The rise in information theft and attack is best understood as part of a more general problem of the exploitation of information systems by criminals. Poorly defended technology is increasingly easy to exploit for fraudsters with ever more advanced tools of their own, ranging from sophisticated hacking to a simple memory stick that can let a disgruntled employee walk into the office and walk out with details of the company's most valuable intellectual property. Of course, not all information theft is digital. Mishandled paper can reveal as much as mishandled data files. Nevertheless, the pervasiveness of information systems shapes the context of the theft.

This year's survey shows how far technology has become an issue for those fighting fraud. Respondents report that the complexity of information infrastructure is the single most

widespread factor in raising exposure to fraud, cited by 28%. Moreover, when respondents were asked which of a series of 10 elements were involved in frauds they had suffered in the last year, the two most common elements were technology-related: phishing attacks (20%) and the increased use of technology (18%). As elsewhere, this is a cross-industry issue – these two responses were the top answers in five of the 10 sectors surveyed. Anonymous email allegation, another increasingly common fraud element, will be closely observed as a result of the new US Dodd Frank Act, which requires the Securities and Exchange Commission (SEC) to reward whistleblowers.

This growing technological challenge, however, is not eliciting as large a response as might be expected. In the coming 12 months, 48% of companies expect to spend more on information security. Although that figure makes this the most common field of anti-fraud investment, it is actually down from 51% from last year.

### Fear of fraud is dissuading a significant number of companies from going global

In the survey, 48% of respondents indicate that fraud has deterred them from engaging in business in at least one foreign country. Nearly two-fifths (39%) of respondents list at least one type of fraud that had dissuaded them from doing business in a foreign market, and 36% name a country or region where their experience or perception of fraud had deterred them from operating. The issue affects small and large companies alike. The breakdown of respondents by revenue for those companies which fraud had dissuaded from investing was the same as that for the survey as a whole.

This is not merely a developing world problem: 7% of those surveyed say that fraud has dissuaded them from operating in North America. Nevertheless, its biggest impact is on emerging economies. Fraud has deterred 11% of those surveyed from doing business in China and Africa, and 10%, in Latin America. These respondents manage risk by simply staying out of these three regions, even though they may present a large investment opportunity.

Moreover, developing countries appear to have more issues to clear up. In our survey, respondents were asked to rank the types of fraud that had dissuaded them from entering certain markets. Twice as many types were

Chart 1. Percentage of companies reporting indicated frauds in the previous 12 months

	2010	2009
Information theft, loss or attack	27.3%	18%
Theft of physical assets or stock	27.2%	28%
Management conflict of interest	19%	20%
Vendor, supplier or procurement fraud	15%	12%
Internal financial fraud or theft	13%	14%
Financial mismanagement	13%	12%
Regulatory or compliance breach	12%	17%
Corruption and bribery	10%	12%
IP theft, piracy or counterfeiting	10%	8%
Money laundering	6%	3%

Chart 2. Percentage of companies within industry reporting information theft, loss or attack

	2010	2009
Financial services	42%	24%
Professional services	40%	27%
Technology, media and telecoms	37%	29%
Retail wholesale and distribution	26%	19%
Consumer goods	25%	22%
Natural resources	22%	27%
Construction, engineering and infrastructure	21%	23%
Healthcare, pharmaceuticals and biotechnology	19%	21%
Travel, leisure and transportation	18%	23%
Manufacturing	13%	23%

listed for developing regions than for North America and Western Europe. Globally, the leading worry is corruption. It has dissuaded 17% of all businesses – and 37% of those who have in fact been deterred – from investing somewhere. Consistent with the other findings in the survey, information theft is also an important concern, ranking second with 9% of all respondents and 19% of those deterred citing it as the reason not to invest.

Although corruption is the most important deterrent to investment in every region, the impact is far from universal. Corruption was named by 63% of respondents as the main reason for not doing business in Africa and by 59% for avoiding Central Asia. By comparison, only 21% of those who were dissuaded by fraud from doing business in

North America list corruption as a leading reason. In most geographies information theft is the second biggest deterrent to investment, but that varies widely, from 7% in Western Europe to 31% in neighboring Central and Eastern Europe. China, where fraud deterred the most respondents, faces a range of challenges rather than a single, overwhelming issue. Corruption and information theft are the two most widespread issues (34% and 33% respectively), but concerns about intellectual property, a long-standing worry for those operating in the country, were a leading factor for 23% of businesses dissuaded from doing business there.

Clearly, many companies are willing to go into emerging markets knowing the risks: 21% believe that their exposure to fraud has

increased because of entry into new, riskier markets in the last year. The survey also found, however, that fraud is exacting an economic price by causing companies to pass on potential opportunities, especially in underdeveloped and emerging economies.

### Companies are unprepared for increasing regulatory efforts against corruption

The Foreign Corrupt Practices Act (FCPA) used to be a quiet backwater for United States law enforcement officials. Those days are now long gone. Between 2005 and 2009, the US Department of Justice brought more than 60 FCPA cases – more than during the entire period from 1977 to 2005. Every sign points to continued acceleration of this trend: early in 2010, 130 open cases were under investigation, their targets ranging from large corporations to small private concerns. American authorities have even begun using sting operations as an FCPA enforcement tool.

This development has global consequences. Not only does the Act cover foreign activity by US persons and companies, it defines the latter category very broadly. Of the 47 fines handed out in 2008 and 2009, 19 hit non-US companies. Operations, share listings, American Depository Receipts (ADRs), and even having United States nationals as board members can potentially open companies up to liability for actions anywhere in the world. Siemens, for example, reached a settlement for activities in South America with the Department of Justice (DOJ) and BAE Systems for behavior in Africa.

Meanwhile, the reach of the UK's new Bribery Act is in theory longer and wider than that of the FCPA, covering the global activities of every person or company doing any business in the UK. It not only prohibits bribery, but covers failure to prevent bribery by persons associated with the company anywhere in the world in both the private and public sectors. UK authorities are unlikely to be any less vigorous than American ones in enforcement of their laws.

The survey indicates that too few companies fully understand the current regulatory situation. Businesses with a link to the United States or United Kingdom are very likely to fall under one of these acts. However, of respondents whose firms had operations or a presence in one of these countries, only 36% believe that these laws applied to them; more than one-quarter believe that they would not, and 37% were not sure. Smaller companies



might have more excuse, but the figures for the largest firms are not much better. For those with annual sales of over \$10 billion, 43% understood that they were covered by one of the acts, and 30% were uncertain.

Not surprisingly, then, only a minority of companies are addressing the regulatory risks that accompany more vigorous FCPA enforcement and the advent of the Bribery Act. Among respondents with operations or a presence in the United States or UK, only one-third believe that their senior managers are thoroughly familiar with the legislation. Just 42% say that they have assessed the risks and set in place the necessary monitoring and reporting procedures. Most of the rest are uncertain, but about one-quarter (24%) say that they have not. Finally, fewer than one-half (47%) are confident that they have the controls in place to prevent bribery at all levels of the operation, and 16% of respondents are sure that this is not the case.

Just because a company knows that it is subject to the FCPA or Bribery Act, it does not automatically follow that it is fully-equipped to comply with them. Of the respondents who believe that one or both of these laws definitely applies to their firms, only 40% say that their senior management understands them, and 32% believe the opposite. While 46% say that their company has done a detailed assessment of their exposure to risks associated with non-compliance to the acts, 29% report that they have not. The only real difference between those who know they are subject to the legislation and the rest of the survey seems to be a greater tendency to steer clear of the problem. Companies with links to either the United States or the United Kingdom need to review their legal position and controls in order not to fall afoul of more aggressive anti-corruption enforcement.

### Fraud is most often an inside job

Employees are the people who have the best knowledge of a company. Unfortunately, this also means that dishonest employees know what there is of value, how it is protected, and the best way to circumvent that protection. In our survey, for those companies that have been affected by fraud in the last year and the culprits identified, the most common fraudsters are equally junior employees (22%) and senior ones (22%). When agents and intermediaries (11%) are added in, the proportion of fraud carried out by those who work for the company in one way or another goes well above half.

The finding is remarkably consistent across geographies, with the proportion of frauds carried out by agents, junior or senior employees falling between 50% and 60% in North America, Europe, and Asia-Pacific. It hits its highest figure at 71% in the Middle East and Africa, and the lowest it goes is only 42% in Latin America, where customers are the single biggest fraudsters. Similarly, that proportion also falls within the 50% to 60% range for most industries, the only exceptions being consumer goods (45%), construction (46%), and professional services (72%).

Some differences between industries do exist. In financial services, for example, a notably high proportion of customers are key perpetrators of fraud (28% compared to a survey average of 10%). Consumer goods companies, meanwhile, suffer 40% of their frauds at the hands of vendors and suppliers, more than twice the survey average of 18%. The broader message of the survey here, however, is an unpleasant one. Whatever the sector, if a fraud occurs the culprit is more often than not likely to be one of the people working with you.

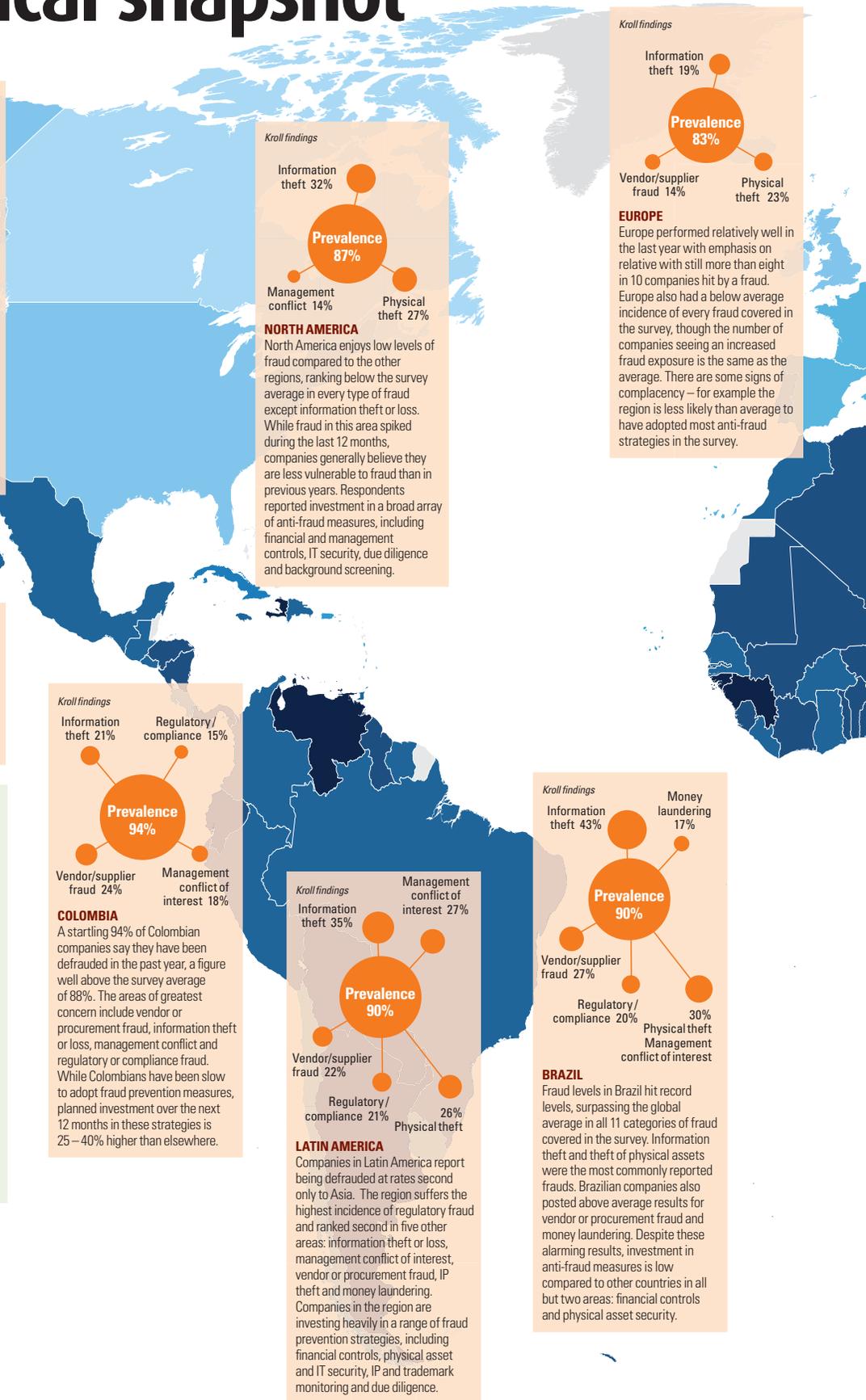
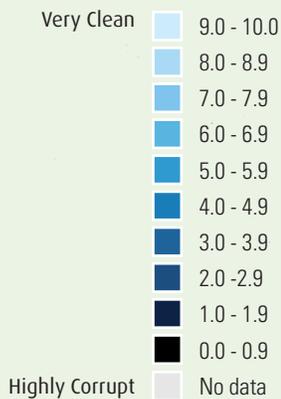
# A geographical snapshot

We compared the results of the Global Fraud Survey findings with Transparency International's Corruption Perceptions Index (CPI). The CPI measures the perceived levels of public sector corruption as seen by business people and country analysts; ranging between 10 (very clean) and 0 (highly corrupt). The comparison clearly demonstrates that fraud and corruption frequently go hand in hand.

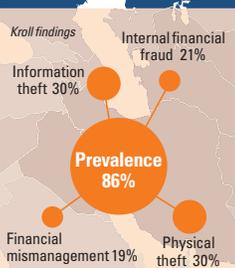
The panels on the map summarize:

- the percentage of respondents per region or country suffering at least one fraud in the last 12 months
- the areas and drivers of most frequent loss

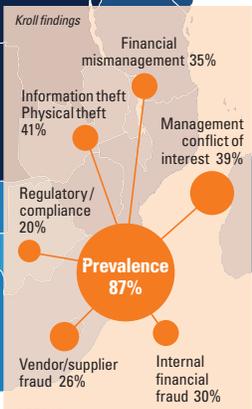
## Transparency International Corruption Perceptions Index 2009



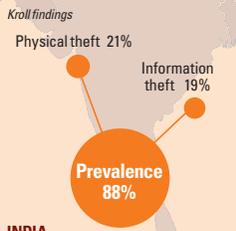
Map image by permission Transparency International. All analysis Kroll/Economist Intelligence Unit.



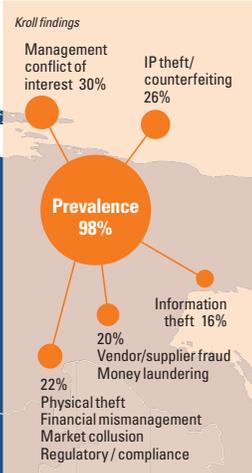
**MIDDLE EAST**  
The Middle East picture is mixed. Below average incidences of fraud in seven of the 11 frauds surveyed is positive, including the lowest levels of vendor fraud, IP theft and conflicts of interest. There are concerning trends emerging however, including higher than average levels of employee theft, the second highest figure for companies suffering at least some financial loss and the highest percentage of respondents that said fraud had grown worse at their companies in the past year.



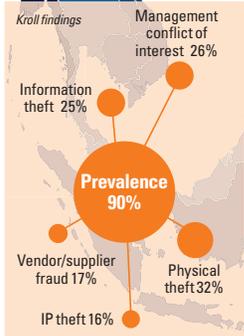
**AFRICA**  
Despite a 1% decline in companies affected by at least one fraud, Africa paints a generally worrying picture. The continent has the highest incidence of fraud in eight of the 11 categories reported and came a close second to Latin America for regulatory and compliance fraud. Africa also saw leaps in the occurrence of fraud through information theft and conflicts of interest. While companies in Africa widely adopt anti-fraud strategies, they do not appear to be working particularly well.



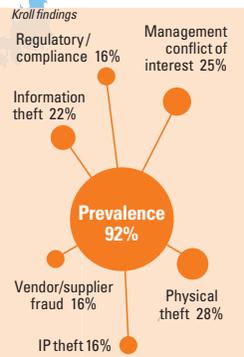
**INDIA**  
Respondents feel mainly vulnerable to regulatory or compliance breach and information theft, loss, or attack, which is not surprising since complexity of IT infrastructure was cited as one of the leading factors contributing to increased exposure to fraud. For those that experienced fraud, 48% reported that the key perpetrators had been their employees. Anonymous email allegations and collusion within the supply chain were involved in 26% and 19% of frauds experienced.



**CHINA**  
Ninety eight percent of respondents in China fell victim to fraud in the last 12 months. The types of fraud are highly varied, with at least one in five companies hit by nine of the 11 frauds covered in the survey. Businesses are doing little to protect themselves: only 54% will invest in staff training and 42% in employee background checks.



**SOUTHEAST ASIA**  
Respondents from the area reported one of the highest rates of theft of physical assets or stock (32%) and face above average levels of management conflict of interest and vendor fraud. While more firms than average are making investments in anti-fraud measures, 35% are weakening controls in order to save money – the highest level for any region.



**ASIA-PACIFIC**  
Asia-Pacific has the highest number of companies being hit by at least one fraud in the last year, with the majority feeling vulnerable to vendor, supplier or procurement fraud or information theft, loss or attack. More worrying is how many companies are looking to cut costs by weakening controls: 33% of firms reported that this practice had increased fraud exposure, up from just 19% last year. High staff turnover was another factor.

# The regulatory challenges of crossing new frontiers

By Tommy Helsby

One result from the latest EIU Global Fraud Survey—that the greatest fraud risk to companies lies with employees and agents—reinforces a truth well-known to practitioners: it's usually an inside job. The prominence of theft of information and electronic data in our survey makes the problem worse: insiders generally have freer access to the valued information. But there is a double risk from employees committing crimes that seek perceived easy routes to business success, such as paying bribes, colluding with competitors and cutting corners on compliance: not only does the company suffer the economic consequences of their behavior but it also opens itself to increasingly robust treatment from regulators. These risks have been heightened by the current economic climate.

Many companies operating in the currently flat markets of the developed world are seeking growth elsewhere, sometimes simply to survive. That is likely to require developing new product lines or entering new geographical markets – which generally means operating outside existing comfort zones. The quick route is to use acquisitions, joint ventures, or distribution agreements but, as with all short cuts, these can be risky. Acquisitions or partnerships can infect a business if they have questionable business practices or lax standards. These may even be perceived to be tolerated in the target's or partner's sector or country of operation, but they can leave the unaware open to economic damage and increasingly harsh treatment from regulators.

This risk is heightened when the move is into an emerging market, where growth rates are higher but governance, compliance and transparency are often less mature than in developed countries and where regulation is sporadic and inconsistent, even arbitrary. Too often, corporate attention focuses on market and credit risk in emerging markets: operational risk is neglected until it turns around and bites you.

## The new regulatory environment

The bite is as likely to come from regulatory enforcement at home as in the place where the offense occurs. Stung by criticism that their laxity contributed to the financial crisis, regulators are acting with renewed vigor, authority, and political backing – and in some cases new legal powers. Certain longstanding prosecutorial backwaters have bubbled into life. The most obvious is corruption: as the Economist Intelligence Unit's introduction highlights, there have been more prosecutions under the United States Foreign Corrupt Practices Act (FCPA) in the past five years than in the previous 30 and the UK has passed a new Bribery Act. Corruption is not the only area of increased regulatory activity: last year fines – in one case of more than half a billion dollars – were levied against several major banks for financial sanctions compliance failures that might once have been seen as little more than clerical errors.<sup>1</sup> Meanwhile, European Union competition investigators have conducted dawn raids to gather documents and the resultant suits have led to fines of hundreds of millions of euros.

Another feature of the new regulatory landscape is the rise of extraterritoriality: the application of laws from one country to actions in another. The FCPA always applied to overseas actions, as does the new UK Bribery Act. So, typically, do competition legislation and trade sanction-related laws. The exposure is not only to the actions of a company's own employees: regulators have gotten wise to the practice of "outsourcing" wrong-doing to a local partner or agent. The UK Bribery Act makes quite explicit a corporation's liability to third party acts that benefit the company, but it has been implicit in most such national legislation already. The onus is now clearly on the company to police the actions of affiliates, partners, and agents, and to have a clear record of doing so, in order to protect its own integrity. This applies not just to the prevention of corruption but to many other aspects of international trade and business regulation.

Regulation has caught up with globalization in other ways as well. Prosecutors and regulators are actively cooperating across borders as never before. In our work, we may find the victim of a fraud in one country, the crime scene in a second, the perpetrator in a third, and the money stashed in a fourth. Putting together effective enforcement across multiple borders used to be a nightmare for legal authorities. The fight against the funding of international terrorism, however, has fostered much better communication between the appropriate institutions in countries, which has in turn permitted dialogue on fraud and corruption investigations.

The embracing of technology by business has also given investigators some powerful tools. Copies of documents, drafts, comments, and circulation lists often remain forgotten on servers; emails may seem to have been killed but their digital ghosts linger on; telephone records and voice mails are stored longer than many realize. The ability to reconstruct an electronic record of a supposed conspiracy has become all too apparent in many high profile investigations in recent years.

## Addressing the risks

This is how a perfect storm builds. Companies need to expand beyond where they have experience and effective controls, but the best opportunities are often precisely in places where these are most needed. Meanwhile, penalties for regulatory failure, and the chances of getting caught, are growing quickly. It is no surprise that almost half of the respondents in the Global Fraud Survey indicate that they have been dissuaded from operating in one or more countries because of fraud risk.

If just staying at home is not an option, though, you can take useful precautions. First, reassess the range of your regulatory exposure. This involves managerial as much as legal analysis: carefully review all of your business processes – including in the finance, IT, marketing, and even the legal and compliance departments – against a list of regulated actions – such as

hiring an agent, making a payment, recording an individual's name, or negotiating with a competitor – and a list of countries where you have any activity. The latter should not be restricted to where you have a physical presence: sales agents, or critical suppliers, for example, may create regulatory exposure. From this matrix, you can begin to develop your global compliance footprint.

When Kroll facilitates these exercises for clients, the results can be alarming. Even if you have just a *de minimis* presence in Ulan Bator and your contact there says that Mongolian anti-competition regulation is lax, you may still be at risk at home. The analysis needs to be dynamic and intelligent: the process driven exercise that many Sarbanes-Oxley compliance reviews became may not suffice.

The point of this exercise is not to develop compliance programs that prevent any of the multitude of identified vulnerabilities from ever becoming a problem. Apart from being cost-prohibitive, this would prevent you from doing almost any useful business anywhere. What you do need is effective contingency planning, having identified the types of responses that may be necessary. Who will make the decisions? Do you have the necessary resources in-house? If not, have you identified and pre-qualified outside assistance in case you need help in a hurry? Do your outside resources match the needs you have now identified, particularly regarding global coverage and relevant experience? Can your team – in-house and external – help you find specialized expertise such as Ulan Bator's top anti-trust lawyer?

There is a hierarchy in crisis management: an issue becomes a problem; the problem develops into a drama; and the drama turns into a crisis. It need not be that way, despite the fraud risks of entering new sectors and markets. Identifying these risks and planning for the consequences eliminates or reduces many surprises, and without surprise, there is no drama. Without drama, an issue is just a problem, not a crisis, and problems are what companies deal with every day.

1 <http://www.guardian.co.uk/business/2010/aug/18/barclays-sanctions-us-court>



**Tommy Helsby** is Chairman of Kroll Eurasia based in London. Since joining Kroll in 1981, Tommy has helped found and develop the firm's core due diligence business, and managed many of the corporate contest projects for which Kroll became well known in the 1980s. Tommy plays a strategic role both for the firm and for many of its major clients in complex transactions and disputes. He has a particular interest in emerging markets, especially Russia and India.

## Regulation: Does awareness match potential impact?

### I agree with the following statement

47.2%

We have set in place adequate procedures to prevent bribery at all levels of our operations

32.9%

Our senior managers are thoroughly familiar with the new UK Bribery Act and the FCPA

26.2%

We do not have sufficient links with the UK or US for these laws to apply to us

Perhaps the most surprising set of responses in the survey related to the potential lack of awareness of the extraterritorial nature of international corruption regulation, given the publicity surrounding both high profile US Department of Justice prosecutions under the FCPA and the introduction of the UK Bribery Act. Close to 70% of respondents have operations or a presence in the UK or US, potentially exposing them to one or both sets of regulations. The responses to three questions in particular stood out:

- How familiar are senior management with the regulations?
- Have you set in place adequate procedures?
- Do you have a sufficient link to the UK/US to be impacted?

As the survey indicates, too few companies fully understand the impact and implications of these laws. Among respondents whose firms have operations or a presence in one of these countries, only 36% believed that the laws applied to them while more than 25% believed that they did not and 37% were not sure.

Companies with operations in regions more prone to corruption need to take particular care: the Securities and Exchange Commission (SEC) recently announced its intention to focus on business in Asia-Pacific, and companies around the world will soon begin to grapple with the limitations imposed by the UK Bribery Act. The survey findings highlight the need for a proactive response to combat potential violations: less than half of those surveyed believe they have adequate bribery prevention procedures in place; 17% say they do not and 25% believe that their companies are not impacted by either law.

Given the survey findings concerning awareness levels, it is less surprising that only a minority of companies are addressing the regulatory risks that accompany more vigorous

FCPA enforcement and the advent of the UK Bribery Act. Fewer than one-half (47%) of those surveyed are confident that they have the controls in place to prevent bribery at all levels of the operation, and 16% of respondents are sure that this is not the case. But just because a company knows that it is subject to the FCPA or UK Bribery Act, it does not automatically follow that it is fully equipped to comply with them.

In Kroll's experience, the impact of anti-corruption legislation is being considered within compliance and legal functions of most organizations, but anti-corruption programs have not generally been fully implemented. Organizations should ensure that a corruption risk assessment has been carried out across their businesses considering both the inherent and residual risk of corruption. A corporate anti-corruption policy and code of ethics should be developed and implemented and must contain a clear statement of an anti-corruption culture fully and visibly supported at the highest levels in the business.

It is important that individual accountability is established for anti-corruption efforts and that training has been implemented and monitored to ensure dissemination of the anti-corruption policies, rules and culture to staff at all levels.

Proactive implementation of an effective anti-corruption program is a minimum requirement in mounting a defense against corruption allegations from regulators and it is imperative that due consideration be given to the reach, financial penalties and reputational impact of anti-corruption regulation.

Penalties imposed by regulators for breaches frequently have a larger financial or reputational impact than the bribe or fraud itself.

# Facing the fraud challenges of emerging market entry



By Melvin Glapion

This year's Global Fraud Survey found that fraud concerns had dissuaded 48% of respondents from operating in at least one region or country. Those geographies most frequently mentioned were China where 11% had been put off, Africa with 11%, and Latin America with 10%. The leading worry – corruption – dissuaded more than one in six businesses from operating elsewhere: for those who stayed away from Africa, it was a concern of 63%, and for Central Asia 59%.

It is surprising to Kroll that nearly half of firms surveyed think that the best way to mitigate fraud risks in some key growth markets, given the potential opportunities available and Foreign Direct Investments (FDI) forecasts, is to avoid them altogether. Indeed, the markets expected to exhibit the highest levels of growth over the next five years are those where fraud is causing the most companies to steer clear. Average compound annual real GDP growth rates in the G7 over the next five years are expected to be below 2%. In comparison, the figure for the BRICs (Brazil, Russia, India, China) over the same period is predicted to exceed 7%.

To examine the link between fraud and investment in emerging markets further, we compared, for a range of countries, the forecast five year growth in stocks of inward FDI – a measure of total investment in local businesses by foreign investors – with the Transparency International Corruption Perception Index (CPI) scores for 2009. We used the latter rather than Global Fraud Survey data both because it contains more detailed country level data and because corruption is the leading fraud impeding investment. As the figure opposite demonstrates, across our entire sample, only the United Arab Emirates combined a greater growth in FDI than the G7 states with a comparable CPI score to the G7 average. All other countries with higher than average FDI growth did significantly worse in the CPI.

Of course every investment involves some level of risk and reward. The perceived levels of corruption within the BRIC countries, which have drawn much of the world's FDI in the last ten years, have actually grown worse. Moreover, those developing countries in the next tier of interest for investors, such as Angola, Ukraine, and Egypt, have even poorer CPI scores.

This growing risk is compounded by increased regulatory oversight of activities in developing and emerging markets. The United States Department of Justice is aggressively enforcing the Foreign Corrupt Practices Act (FCPA), and the UK's new Bribery Act has extra-territorial reach, strict liability, third party responsibility, and a ban on facilitation payments. A serious concern is how few companies seem to realize that they may come under greater scrutiny or face higher penalties. As page 11 highlights, the Global Fraud Survey found that only 36% of respondents who had operations or a presence in the UK or the US thought that they could be prosecuted under the FCPA or the Bribery Act.

The dilemma is difficult: going into many emerging markets leads to significant fraud risk exposure but staying out means sacrificing growth prospects that are absent in developed countries. The latter could also mean being left behind as competitors seek to establish positions in what will be among

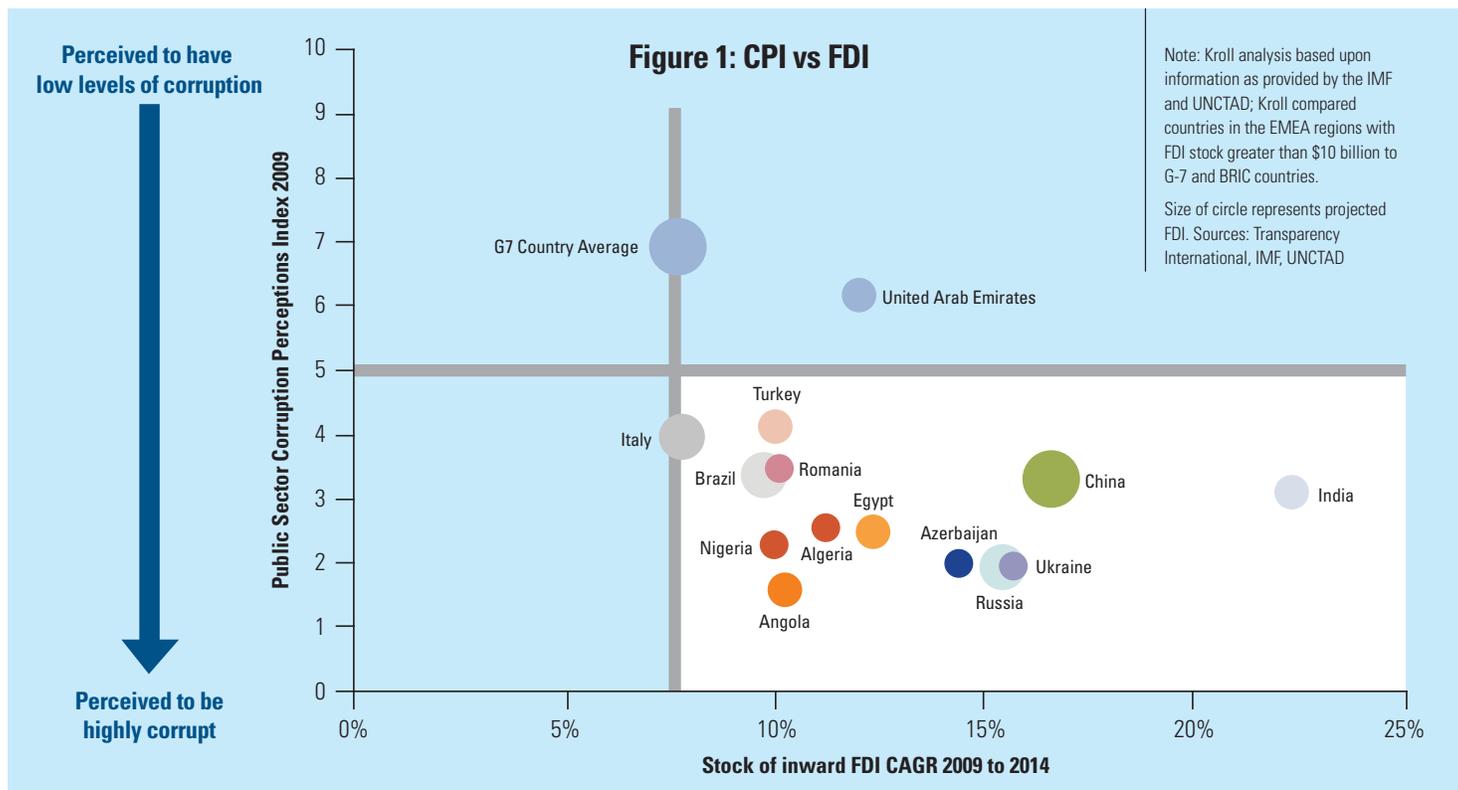
the leading markets of the future. Is there a way to enter these dynamic but challenging economies yet mitigate the obvious risks?

## Due diligence in challenging markets

Those considering the plunge could begin by accepting that conducting due diligence in this environment needs to be done differently. Whether entering a new market through acquisition or joint venture, or contracting with a distributor or supplier, financial and legal due diligence remains essential but on its own will be insufficient, picking up only documented instances of fraud.

A more effective approach is to combine commercial and integrity due diligence into a unified whole which also takes account of the difficulties created by several fundamental differences between emerging and developed markets:

- **The quality of the secondary information:** In emerging countries, industry reports, brokers' notes, or guidance from chambers of commerce or trade associations are often inaccurate or nonexistent. Assessing the size, structure, and segmentation of these requires a balance of desktop research and intelligence gathering in the field.
- **The political/regulatory environment:** Commerce and politics are interconnected and investigating potential conflicts



should be a high priority before investing significant time and resource in a country. Our investigations in emerging markets, for example, often uncover opaque relationships between customers, suppliers, and local officials. Also vital in this sphere is gaining an understanding of the robustness of the local government and regulatory bodies, as well as of what changes might occur after an investment takes place. There are several unfortunate examples of companies investing millions of dollars only to have licenses revoked by a new regime months later.

- **The need for physical searches and human intelligence:** In many of these countries, certain key information is held locally and in physical form. Moreover, members of the business and financial communities are more likely to express true opinions or give advice only in person and to someone they know.

Once companies appreciate the challenges of doing due diligence in these markets, what specific steps should they take before market entry? Despite the inevitable limits on what can be done pre-deal or pre-partnership, some sensible steps include:

- Ensure that your board shows commitment and leadership in order both to drive home the importance of anti-fraud programs and to avoid potential liability for negligently failing to prevent fraud;

- Involve internal or external counsel in a review of all key strategic options in order to ensure that commercial opportunities are assessed against fraud risks;
- Safeguard against unforeseen risks. Companies should seek to include deal terms that are even more defensive than usual when dealing with partners or purchases in riskier jurisdictions;
- Ensure that anti-fraud programs are embedded within your organization and extend to the company's intermediaries and partners. Significant investment will be required in communicating these policies as emerging market countries typically do not have a culture of "whistleblowing".

Although this advice applies to all types of fraud, companies should, given the particular risks at present, pay special attention to implementing them with respect to anti-bribery and anti-corruption efforts.

Perhaps the most difficult advice for companies to adopt, given the speed at which transactions now take place, is to allow enough time for this commercial and integrity due diligence. Early planning can avoid the significant costs on potential transactions that, in the end, prove inappropriate. Initial due diligence work should: analyze the size of the opportunity; identify the touch-points for potential fraud; and, what is often forgotten, be broad enough to consider alternative options.

Kroll was recently approached to review a potential partner for a global energy company seeking to enter the Chinese market. The call came one month before an agreement was to be signed. Through painstaking research and discreet human source inquiries, Kroll concluded that the proposed partner had significant issues with respect to its financial, operational, political, and environmental performance. The energy company, which had initially expected a clean bill of health, was in the unwelcome position – after several months of staff time, travel expenses, and advisors' fees – of trying to find a more suitable partner. An integrated due diligence exercise that had begun earlier would have saved time and money.

Due diligence, however, should never end with the acquisition. In the following article Glen Harloff and John Price discuss options when the acquisition raises concern post-competition.



**Melvin Glapion** leads Kroll's business intelligence practice in London. He has over 16 years of experience of M&A, corporate strategy and financial analysis experience, leading multi-disciplinary and multi-jurisdictional teams in conducting cross-border market entry, due diligence and competitive intelligence engagements. Previously he advised on corporate strategy initiatives at KPMG, and has held several other strategy roles within the private sector.



**This year's Global Fraud Survey reveals that fraud has dissuaded 48% of respondents from entering new markets. The risk of uncovering questionable behavior post-acquisition is a likely driver of this figure. What are your options when an acquisition in unfamiliar territory raises suspicions?**

**By Glen Harloff & John Price**

Only so much can be investigated by lawyers and accountants during a typical due diligence period. A truer picture, including questionable links between management and a company's vendors or customers, often only comes to light post-transaction when the new management team is in full possession of the facts, accounts and records. The changes brought about by a purchase may even induce fraud. Occasionally, financial investors or a foreign strategic buyer acquiring a privately held business will use carrots, such as bonuses tied to aggressive profit goals, or sticks, such as terminations in the event of poor results. These can place managers under unaccustomed, intense pressure to perform which may tempt certain sub-par staff to adopt fraudulent practices.

For example, a publicly traded retail company recently acquired a well-established retail operation in a foreign jurisdiction. One of the latter's main attractions was the CEO, who had a stellar reputation. The buyer provided additional incentives, tied to certain revenue and profit goals, to the CEO and his senior management team. After the second quarter, the CEO realized that these targets would not be met. Perhaps, as we see frequently in such cases, pride and greed took over, but instead of reporting the true financial results, the CEO, in collusion with the CFO and other senior managers, "cooked the books." Sales were overstated, expenses understated or inappropriately capitalized. Two years later, an anonymous e-mail resulted in an investigation which uncovered the fraud, but by then the damage was done – and the bonuses distributed.

# Preventing fraud in new acquisitions

Kroll has seen a number of ways in which valuations pre-deal can be manipulated.

For example:

- A disgruntled or under-performing manager might also sell intellectual property – such as customer lists or proprietary formulas – or company assets that are gathering dust to the competition.
- He might start a new company, disguising its true ownership, and divert customers to it or sell overpriced services back to his employer.
- A dismissed manager might set up his own firm using the customer data from his former employer, as non-compete contract clauses are often extremely difficult to enforce. Indeed, as the Global Fraud Survey reports, management conflict of interest, including related-party transactions, has affected nearly 20% of companies worldwide.

For buyers, all is not lost. Everyone anticipates a thorough house-cleaning during the first six months after a take-over. This is the ideal opportunity for a detailed review of the firm's financial integrity and a search for fraud, as per the steps to the right. It is also the time to shore up operational vulnerabilities, including those managers who have been proven to be unethical.

It is best practice for the internal audit function to review an acquisition post purchase. It also makes commercial sense to instruct external forensic or financial investigators where the geography or industry sector is less familiar to the internal team. Additionally, where an extra layer of independence and expertise in both identifying fraud and understanding how your systems were defeated is essential, a forensic investigator is often best placed to advise you on next steps.



**Glen Harloff** (CGA CFI) is a managing director based in Kroll's Miami office. He is an expert in financial investigations and has extensive experience in the prevention, detection and investigation of fraud for clients throughout the Caribbean and Latin America.



**John Price** is a managing director based in Kroll's Miami office. He specializes in business intelligence in Latin America and serves as a strategic advisor to clients on competitive positioning, market entry, transactional due diligence, competitive intelligence and business risk analysis.

## Steps for new owners to uncover or prevent fraud

- Conduct a detailed review of sales and accounts receivable. This includes meeting the top customers in order to understand their purchasing and payment patterns.
- Get to know who your suppliers are and how they are structured. Look closely at any smaller ones that conduct more than 20% of their business with your company.
- Review related-party transactions, especially the links between key internal managers and the ownership of key vendors.
- Conduct background checks on any second-tier managers who may have been overlooked in pre-transaction due diligence but who preside over key functions that are vulnerable to fraud, such as IT, finance, payroll, warehousing, and security.
- Put in place appropriate internal controls.
- Conduct regular reporting, either weekly or monthly, and look into reports that identify unusual but significant events. Do not rely on year-end financial results: these are typically too high level and arrive too late.
- Insert trusted and competent managers into key managerial positions, especially that of CFO, but then monitor them just like any others.
- Although post-deal integration will be a priority, it may be helpful to keep separate operations initially while you evaluate and investigate areas of concern.
- If you find evidence of criminal activity, upon the advice of counsel, contact the authorities and co-operate with any necessary investigation. Also modify procedures where necessary and maintain records of communicating known or alleged instances of fraud. This will help prove a company's commitment to prevention.

### ECONOMIST INTELLIGENCE UNIT REPORT CARD

### RETAIL, WHOLESALE & DISTRIBUTION

The retail, wholesale, and distribution sector saw a reduction in the incidence of fraud, but cost considerations are leaving it exposed to trouble in the future. This sector is facing increased exposure to information theft, loss or attack (26%) and vendor, supplier or procurement fraud (17%) compared to last year. That said, the incidence of information theft rose, but for eight out of 10 types of fraud there was a decline in the proportion of companies affected. Similarly, although the industry had the second-highest number reporting physical theft (41%), it had the lowest percentage for money laundering (0%), regulatory breaches (0%), corruption (4%), and financial mismanagement (4%). The big worry is not last year's results, but the growth in fraud exposure. The sector has the highest proportion of firms where staff turnover (37%), pay restraint (24%), and weaker internal controls (24%) are leaving them more open to fraud.

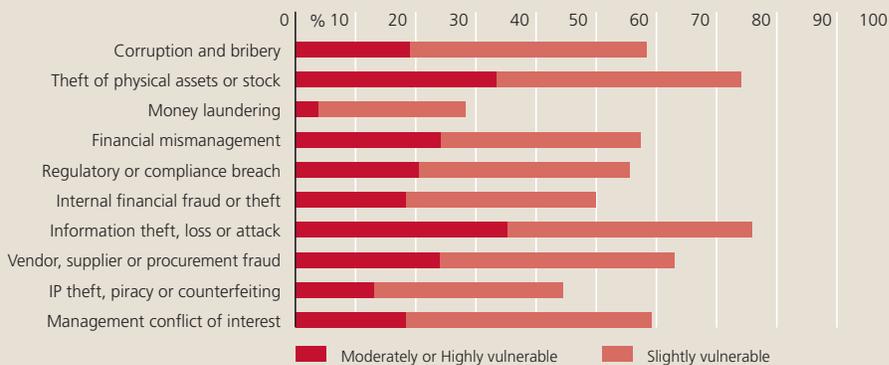
**Prevalence:** Companies affected by fraud 86%

**Areas of Frequent Loss:** Percentage of firms reporting loss to this type of fraud  
 Theft of physical assets or stock (41%) • Information theft, loss or attack (26%)  
 Vendor, supplier or procurement fraud (20%) • Management conflict of interest (17%)

**Investment Focus:** Percentage of firms investing in prevention of this type of fraud;  
 IT security (59%) • Financial controls (54%) • Physical asset security (52%) • Management controls (50%)  
 IP and trademark monitoring program (48%) • Due diligence (46%) • Risk management systems (43%)  
 Reputation monitoring (43%)

**Increase in Exposure:** Companies where exposure to fraud has increased 80%

**Biggest Drivers of Increased Exposure:** Most widespread factor leading to greater fraud exposure and percentage of firms affected; High staff turnover (37%)



# NORTH AMERICA OVERVIEW

Fraud levels remain low in North America compared to other regions in all areas except one: information theft or attack. According to this year's results, fraud in this area rose to 32% from a more modest 19% last year. The significantly high levels of information theft reported exceed the survey average of 27%. Notably, North American respondents cited phishing (26%) and the increased use of technology (19%) as the primary tactics used in this type of fraud. When probed further, 26% of those surveyed cited the complexity of IT infrastructure as the leading cause of increased fraud exposure.



The growing threat to information security, however, may not be getting the attention that it deserves. Only 34% of respondents considered themselves moderately to highly vulnerable to information theft. Moreover, investment in IT security measures declined this year versus last.

Overall, companies in the region believe they are less vulnerable to fraud. They also report low exposure in areas such as corruption (7%) and market collusion (4%). In spite of this, the challenge still remains for businesses to recognize the potential risks of violating the US Foreign Corrupt Practices Act (FCPA). Only 42% of respondents were certain that the FCPA applied to them while 44% were unsure and 14% believed it does not.

North American companies currently enjoy a relatively benign fraud environment. They will need to address growing risks, especially in information security, to keep things that way.

	2010	2009
<b>Prevalence:</b> Companies affected by fraud	87%	78%
<b>Areas of Frequent Loss:</b> Percentage of firms reporting loss to this type of fraud	Information theft, loss or attack (32%) Theft of physical assets or stock (27%) Management conflict of interest (14%)	Theft of physical assets or stock (22%) Information theft, loss or attack (19%) Management conflict of interest (17%)
<b>Investment Focus:</b> Percentage of firms investing in prevention of this type of fraud	Financial controls (45%) Management controls (44%) IT security (42%) Due diligence (41%) Staff screening (40%)	IT security (44%) Financial controls (40%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	66%	84%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	IT complexity (26%)	IT complexity (32%)

# DATA BREACH MANAGEMENT: What every company should know

In a true sign of the times, companies participating in this year's Global Fraud Survey reported that information theft is now the most common form of fraud. With 27% of companies reporting incidents within the past year, the theft of information surpassed the theft of physical property for the first time in the four-year history of the Survey. Some industry sectors were particularly hard hit, foremost among them financial services (42%, up from 23% the previous year), professional services (40%, up from 23%), and Technology, Media and Telecoms (37%, up from 15%). And while companies clearly recognize the increasing severity of the problem, to some extent they feel unprepared to deal with it: 77% of respondents believe that their companies are vulnerable to information theft.

By Alan Brill, Brian Lapidus and Richard Plansky

Given the financial, legal, and reputational risks that go hand-in-hand with a data breach, failing to prepare for one is to court disaster. When an incident occurs, there is no time to learn on the fly, so having a response plan already in place is critical. While there is no such thing as a one-size-fits-all response plan, the best plans tend to share common elements. In particular, they are designed to accomplish five key goals:

## 1. Provide the proper resources for early detection

Too often, the first indication that an incident has occurred is a call from a victim complaining that an account has been looted or, worse yet, a reporter writing a story on a breach. A solid plan should contain a strategy for detecting potential problems at the earliest possible stage by integrating technology (e.g. intrusion detection and

prevention systems, log analysis, anomaly analysis) with a robust training regime to ensure that key personnel understand what to look for and what to do when they suspect that something is wrong.

## 2. Determine if the breach event is still happening and then "stop the bleeding"

Too many companies concentrate immediately on the process of notifying victims before they know all the facts. A good response plan should include a clear process for determining – with forensic accuracy – what did and did not happen and whether any of it is still occurring. Many malicious software attacks have, as part of their structure, elements designed to keep the malware in place long after the initial intrusion. This can lead to automated re-infections weeks or even months after a system is thought to be cleansed and the subsequent compromise of additional data. Absent the certainty

that sensitive information is no longer being compromised, it is impossible to mount an effective response.

## 3. Determine the scope of the breach

In the event of a breach, the extent to which data has been compromised is not always readily apparent. In some instances, the situation is far less serious than suspected. For example, reverse engineering of malicious software can sometimes reveal that the malware did not actually work – i.e., an intrusion without the data loss. In other cases, analysis of the criteria by which a malicious software program selects records to target can show that, since fewer records meet those criteria, the loss was much smaller than originally feared. On the other hand, sometimes the loss is more extensive than initial appearances might suggest. Either way, it is vital for companies to discern the universe of compromised information with enough accuracy – and evidence – to justify their subsequent course of action.

#### 4. Determine who is responsible for the breach and attempt to recover lost data

The loss of information sometimes stems from the loss or theft of a physical object – e.g., a laptop computer, USB drive, or disc – often due to the carelessness or misconduct of an employee. In circumstances like this, a good response plan will provide a process and the resources to conduct a solid fact-finding investigation into the circumstances of the loss. A prompt and robust investigation can often lead to the identification of the person or persons responsible for the loss, which can, in turn, result in a more detailed understanding of the extent to which the data has been disseminated. In some instances, the lost information can even be recovered, reducing or eliminating the need for notification.

#### 5. Determine and comply with legal obligations

In the United States, the regulatory regime for data breach is extremely confusing, with different requirements for different industries and different states. With the exception of the Health Information Technology for Economic and Clinical Health Act (HITECH), which contains breach notification mandates for entities covered under the Health Insurance Portability and Accountability Act (HIPAA), there is no overarching federal law governing breach notification. Instead, there is a patchwork of laws from 46 states and two territories. These laws present varying and sometimes contradictory requirements regarding the entities to be notified and the information that can and cannot be included in the notification letters. A good plan will provide the professional resources necessary to clearly determine the nature and extent of the company’s legal obligations and develop a viable strategy for complying with them.

Without question, a well-crafted response plan can go a long way toward mitigating the damage that flows from a data breach. Better yet is to take proactive steps to prevent incidents from occurring in the first place. Some recommended steps are described below:

- **Data Mapping** – It is critical for companies to understand where and in what form their sensitive data is stored. An awareness of where that data resides and how it is transferred both internally and externally can serve as the foundation for sound policies and procedures to mitigate significantly the risk of breach.

- **Vulnerability Testing** – Regular testing to identify vulnerabilities that a hacker or dishonest insider might exploit are also vital. There are excellent tools to do this, although many organizations elect to engage specialists who have a depth of experience in responding to incidents and extensive knowledge of the latest threats.

- **Use Encryption** – Many of the statutes relating to data breach provide for exceptions when the data in question was encrypted. Because of this, the use of encryption, particularly for data in a form frequently associated with data loss incidents – e.g., data stored on portable devices and back-up or archival data stored on tapes – should be considered a best practice. Many application programs also permit data to be encrypted while residing in a database, another practice that provides protection with little added risk.

- **Policy Review** – In a world of rapidly evolving threats, changing legal requirements, and new outsourcing technologies like cloud computing, it is imperative to review policies at least annually.

Given the current trends, there is every reason to expect next year’s survey to show an even higher prevalence of information theft. With some smart advance planning, there is every hope that companies will be better prepared.

**Alan Brill** is a senior managing director at Kroll Ontrack, where he founded the computer forensics practice. With more than 33 years of consulting experience, his work has ranged from large-scale reviews of information security and cyber incidents for multi-billion dollar corporations to criminal investigations of computer intrusions. His work also focuses on prevention and investigation of data breaches involving sensitive personal, health and corporate information.

**Brian Lapidus** is Chief Operating Officer, Kroll Fraud Solutions has unique frontline experience helping a wide variety of corporations and organizations safeguard against and respond to data breaches. He oversees a highly skilled team that includes veteran licensed investigators who specialize in supporting breach victims and restoring individuals’ identities to pre-theft status. He also works with consumer organizations to help ensure responsible practices among businesses that provide identity theft-related services.

**Richard Plansky** is a managing director and head of Kroll’s New York office. With 18 years of investigative and law enforcement experience, Richard manages a wide variety of complex assignments with a special emphasis on corporate investigations.

### ECONOMIST INTELLIGENCE UNIT REPORT CARD

### HEALTHCARE, PHARMACEUTICALS & BIOTECHNOLOGY

The healthcare, pharmaceuticals, and biotechnology sector is finding that a shift in business models can change fraud patterns. Partnerships and joint ventures are becoming increasingly common throughout the sector, from early R&D to commercialization. This shows up in the fraud data: information theft and IP theft (both 19%) are now the third and fourth most common frauds, having risen from 10% and 7% respectively last year. Greater collaboration has increased fraud exposure for a quarter of companies, the second-highest figure for any of the sectors in the survey. Moreover, although frauds are still as likely to be inside jobs as in other industries, in 6% of cases the main perpetrator was a partner – the highest rate for any industry. Fortunately, health executives are realizing that they need to pick their friends carefully. The number of those expecting to invest in due diligence in the next 12 months is 45%, up from 29% in last year’s survey.

**Prevalence:** Companies affected by fraud 88%

**Areas of Frequent Loss:** Percentage of firms reporting loss to this type of fraud: Theft of physical assets or stock (34%) Management conflict of interest (21%) • Information theft, loss or attack (19%) • IP theft, piracy or counterfeiting (19%)

**Investment Focus:** Percentage of firms investing in prevention of this type of fraud: IT security (53%) • Staff training (51%) • Management controls (47%) • Due diligence (45%) • Staff screening (45%) • Financial controls (45%)

**Increase in Exposure:** Companies where exposure to fraud has increased 75%

**Biggest Drivers of Increased Exposure:** Most widespread factor leading to greater fraud exposure and percentage of firms affected; Increased collaboration with other firms (25%)



# The SEC cracks down harder on pay to play

By Marcia Berss

Banks have long had “Know Your Customer” rules; now the United States Securities and Exchange Commission (SEC) is telling investment managers to “Know Your Placement Agent” as part of its efforts to crack down on “pay to play” – the practice of making political donations or payments in return for government business.

For investment managers seeking government work, federal, state, and local pension fund investments hold out enticing prospects. These total more than \$2.6 trillion, or one-third of all US pension assets. On June 30 of this year, the SEC adopted rules to restrict investment managers from making political contributions if they are trying to win government business. They also require placement agents – third parties hired by investment managers to solicit government business – to register with the SEC.

The SEC first addressed pay to play in 1999, but recent events show that those rules did not go far enough.

- In March 2009, the SEC charged New York State’s former Deputy Comptroller with

attempting to extract illegal kickbacks from placement agents trying to obtain business from the New York State Common Retirement Fund.<sup>1</sup> The SEC and New York’s Attorney General also charged private equity firm Quadrangle Capital Partners with trying to win a \$100 million investment from the fund by paying more than \$1 million to a top political adviser and fundraiser of the State Comptroller, who oversaw the fund.<sup>1</sup> In April 2010, Quadrangle agreed to pay a \$12 million fine to settle the charges and pledged to support regulators’ efforts to ensure that investment managers are selected “based solely on merit.”<sup>2</sup>

- In 2009, a private investment advisor to New Mexico’s State Investment Council admitted that, due to pressure from unnamed, politically-connected individuals, he had recommended investments which were not necessarily in the state’s best interest. A grand jury is investigating.<sup>3</sup>
- In May 2010, the California Attorney General sued a placement agent, representing leading private equity firm Apollo Global Management, for “attempting to bribe” a senior investment officer at the California Public Employee Retirement

System (CalPERS), the nation’s largest public pension fund. The agent had allegedly sought to persuade CalPERS to buy a 10% interest in Apollo.<sup>4</sup> Apollo was not charged and said it was “deeply troubled” by the allegations.<sup>5</sup>

The SEC had originally considered an outright ban on placement agent solicitations of pension management business but backed down: investment managers complained that they could not get access to pension funds without these intermediaries. Instead, the SEC is requiring for now that placement agents register with it, but has made clear that if they “continue to inappropriately influence the selection of investment advisors for government clients,”<sup>6</sup> it will consider a full ban.

In this environment, private money managers must do their due diligence before they hire placement agents – just ask Carlyle Group. In May 2009, the big private equity firm agreed to pay \$20 million to New York as part of the state’s investigation into the use of placement agents at the New York Common Retirement Fund. At the same time, Carlyle sued its placement agent for more than \$15 million, asserting that it had been “victimized” by an “alleged web of deceit.”<sup>7</sup>

Similarly, trustees of public pension funds should understand the business backgrounds and relationships of placement agents seeking to do business with their funds. United States financial firms should also assess how these rules will impact their business with sovereign wealth funds under the Foreign Corrupt Practices Act.

The recent Global Fraud Survey shows increases in management conflict of interest and compliance breaches among financial services firms. Ten years after the SEC first attempted to address pay to play, though, a new era of transparency and accountability in public finance may have finally arrived.

- 1 SEC Litigation Release 20963 dated March 19, 2009
- 2 SEC Litigation Release 21487 dated April 15, 2010.
- 3 Press release issued by Quadrangle dated April 15, 2010, ‘Quadrangle settles investigations with New York Attorney General and SEC’
- 4 ‘SEC limits investment adviser campaign donations’, the Santa Fe New Mexican, July 2, 2010
- 5 Superior Court of the State of California, County of Los Angeles, West District, The People of the State of California v. Alfred Robles Villalobos, ARVCO Capital Research LLC, Federico R. Buenrostro Jr., et al. Case Number SC107850 filed May 5, 2010, page 18
- 6 Suit cited above plus ‘California sues pension middlemen’, Wall Street Journal, May 7, 2010
- 7 <http://i.marketnews.com/node/15796?>
- 8 <http://www.carlyle.com/Media%20Room/News%20Archive/2009/item10682.html>

## ECONOMIST INTELLIGENCE UNIT REPORT CARD

## FINANCIAL SERVICES

Although last year’s survey showed the financial services sector doing badly, in the last 12 months things have grown even worse. For the sector, the incidence of every fraud but one increased, sometimes substantially: those reporting theft of physical assets nearly tripled (from 12% to 33%). In particular, financial services had the most widespread problems with information theft (42%), internal financial fraud (31%), and regulatory breaches (25%). The sector is also the most worried about these three frauds (57%, 51%, and 51% respectively of companies report themselves at least moderately vulnerable). Sector respondents also are the most vulnerable to management conflict of interest (52%), financial mismanagement (47%), and money laundering (51%).

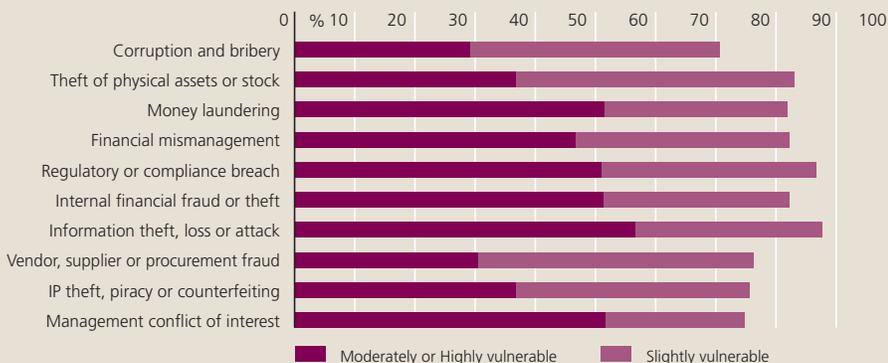
**Prevalence:** Companies affected by fraud: 87%

**Areas of Frequent Loss:** Percentage of firms reporting loss to this type of fraud:  
Information theft, loss or attack (42%) • Theft of physical assets or stock (33%)  
Internal financial fraud or theft (31%) • Regulatory or compliance breach (25%)  
Management conflict of interest (20%) • Financial mismanagement (16%)

**Investment Focus:** Percentage of firms investing in prevention of this type of fraud:  
IT security (47%) • Risk management systems (44%) • Financial controls (42%)

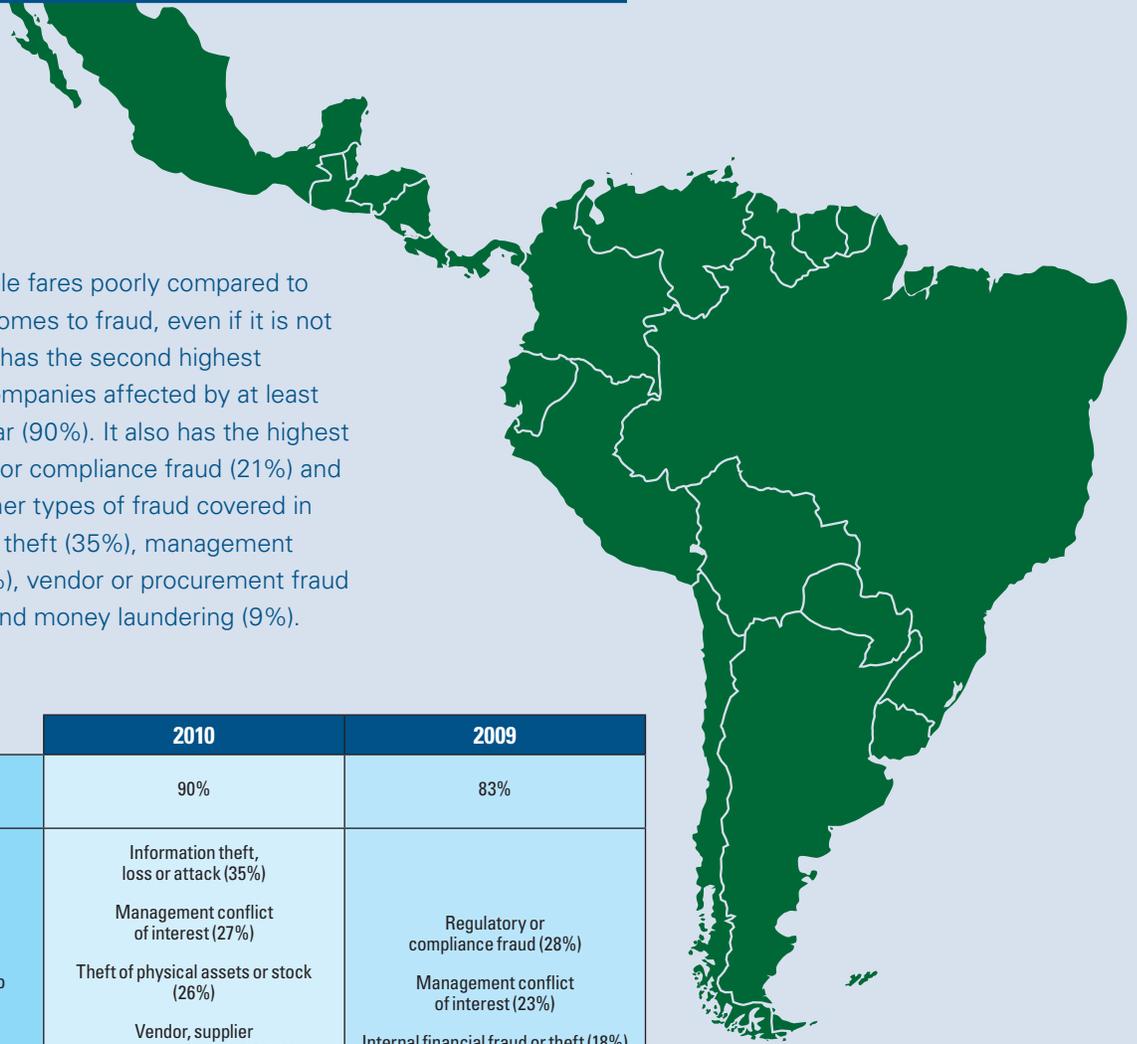
**Increase in Exposure:** Companies where exposure to fraud has increased: 76%

**Biggest Drivers of Increased Exposure:** Most widespread factor leading to greater fraud exposure and percentage of firms affected: IT complexity (43%)



**Marcia Berss** is an associate managing director in Kroll’s Chicago office specializing in public securities filings, corporate finance and corporate governance issues. She began her career as a corporate finance associate with Warburg Paribas Becker and was vice president in M&A for Dean Witter Reynolds.

# LATIN AMERICA OVERVIEW



Latin America as a whole fares poorly compared to other regions when it comes to fraud, even if it is not the worst performer. It has the second highest number after Asia of companies affected by at least one fraud in the last year (90%). It also has the highest incidence of regulatory or compliance fraud (21%) and ranks second in five other types of fraud covered in the survey: information theft (35%), management conflict of interest (27%), vendor or procurement fraud (22%), IP theft (10%), and money laundering (9%).

	2010	2009
<b>Prevalence:</b> Companies affected by fraud	90%	83%
<b>Areas of Frequent Loss:</b> Percentage of firms reporting loss to this type of fraud	Information theft, loss or attack (35%) Management conflict of interest (27%) Theft of physical assets or stock (26%) Vendor, supplier or procurement fraud (22%) Regulatory or compliance fraud (21%)	Regulatory or compliance fraud (28%) Management conflict of interest (23%) Internal financial fraud or theft (18%)
<b>Investment Focus:</b> Percentage of firms investing in prevention of this type of fraud	Financial controls (67%) Physical asset security (57%) IT security (56%) Staff training (55%) IP and trademark monitoring program (53%) Staff screening (51%) Management controls (50%) Risk management systems (47%) Reputation monitoring (47%) Due diligence (46%)	IT security (52%) Financial controls (45%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	85%	72%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	High staff turnover (34%) IT complexity (33%)	IT complexity (37%)

Another serious concern for Latin America is that far more companies report an increase in their exposure to fraud than in other regions. A full 85% of Latin American companies believe they have become more vulnerable compared with 75% of companies in Asia or the global average of just 73%. In fact, more companies in Latin America, 34%, cite high staff turnover as a contributor to fraud. The region also reports the second highest increase in exposure to fraud, after Africa at 18%, resulting from increased collaboration between firms. It trails Asia with 16% of respondents citing more aggressive regulatory enforcement in helping to uncover fraud.

On the positive side, the percentage of companies planning to invest in every one of the anti-fraud measures covered in the survey is also above average and in three cases – staff training (55%), IP monitoring (53%), and due diligence (46%) – the highest of any region. Let’s hope Latin America begins to address the problem.

# Transportation infrastructure fraud in Brazil: STEERING CLEAR OF THE POTHOLES



By Vander Giordano & Allie Nichols

Traveling by air, land, or sea in Brazil can be a feat of epic proportions. The Federation of International Football Association's (FIFA) Secretary-General told the country's authorities that airport facilities and connections between host cities are the Federation's greatest concerns for the 2014 World Cup. The apprehension is well-founded: although the World Economic Forum's *Travel and Tourism Competitiveness Report 2009* ranked Brazil 45th out of 133 countries overall, its airport infrastructure was rated 101st.

The country is also home to some of the world's worst automobile traffic: São Paulo, the largest city, regularly endures traffic jams of over 100 miles long – the longest was 165. The city puts the annual cost of the traffic at \$2.3 billion. The ports are choked with lines of ships as well. Bloomberg reports that trucks delivering sugar wait up to 40 hours to unload their cargo onto vessels.

Brazil must address these problems in order to sustain current levels of economic growth. Of more immediate urgency, however, is the need to be ready for the inundation of tourists expected for the World Cup in 2014 and the Olympics in 2016. In its application to host the latter, for example, Brazil committed to spend \$1.1 billion on upgrades to Rio de Janeiro's suburban railway, \$1.5 billion on projects to expand and connect pre-existing Bus Rapid Transit systems, and \$1.2 billion for metro line extensions. In addition, \$80 million is earmarked for airport upgrades to renew and add terminals and runways and to expand parking facilities in order to accommodate 25 million passengers annually by 2014.

Whatever its immediate cause, such infrastructure investment will clearly provide long-term benefits for the country's population and significant opportunities for investors and companies alike. Investors and project planners, however, must take into account the prevalence and history of fraud that has long tainted this industry in Brazil. The latest Global Fraud Survey suggests this trend continues, having found that 83% of Brazilian companies believe that their exposure to fraud has increased over the last twelve months. The Survey also revealed that 27% of Brazilian companies indicated that they had been the victim of vendor, supplier, or procurement fraud during that time. In the coming wave of investment, the planning, organization, and management of these projects will be critical to determining whether they will be successes or costly failures beset by fraud.

## Two cautionary tales

For years, transportation infrastructure projects in Brazil have been rife with fraud and the problem shows no sign of abating. As recently as August 5, 2010, arrest warrants were executed for 28 individuals accused of rigging bids and diverting funds related to several transportation infrastructure projects in Brazil. Losses are estimated to be nearly \$2.9 million and the accused range from government administrators and officials to owners and employees of the companies contracted to perform the work. They face a wide range of charges, from corruption, embezzlement, and money laundering to forgery, conspiracy, and other criminal violations of Brazilian bidding laws.

Another recent example of fraud in the sector came to light in September 2009 when a whole host of individuals, companies and other entities that provide or manage services related to the air travel industry were investigated

for allegedly rigging online auctions and forming a cartel that served to exclude potential competitors from the market. Of the 305 companies authorized to participate in bids, only 16 actually registered. The fraud, estimated to have reached more than \$286 million, was one of the largest of its kind in recent Brazilian history.

The ways in which fraud in the industry has been perpetrated are seemingly endless: overbilling, overpayments, use of ghost employees, use of materials of inferior quality, attesting to work that has not actually been completed, forewarnings about upcoming audits, altering or concealing documents. Given the widespread presence of fraud, the risks inherent in participating in infrastructure projects can outweigh the benefits. In most cases, these projects involve government officials or entities in some capacity. Consequently, if your company has any significant link to the United States or United Kingdom, the far-reaching provisions of the Foreign Corrupt Practices Act (FCPA) or UK Bribery Act could lead to crippling costs, including penalties, disgorgement of profits, and mandatory monitoring. Moreover, Brazilian authorities can separately impose their own hefty fines and initiate criminal and civil litigation. Finally, conviction for fraud, or even investigation, can result in reputational damage which, while difficult to quantify, will certainly leave a long-lasting scar on any company or individual involved.

**Be prepared**

For companies seeking to exploit upcoming investment opportunities there are several ways to build up a layer of protection against fraud. The first step is to evaluate the transparency and fairness of the bidding process carefully. Some of the key questions that should be asked include: Have the details of the process been clearly communicated? Is an independent committee or person presiding over the process? What criteria will be used to qualify or disqualify bidders? Are these criteria fair or tailored to disqualify all but a select few companies? Are they reasonably related to the necessities of the present project? What factors will be considered in selecting the winner? All of these questions should be answered to the company's satisfaction before it submits a bid.

The second step for a business is to conduct background checks on its own employees and on those companies which it will engage. This is especially important when subcontracting local workers and businesses. A thorough background check can provide clearer details of their qualifications and prior experience, how they are perceived by their competitors and clients, and whether they

have previously been involved in fraudulent projects or have otherwise been the subject of a fraud investigation.

Competitive market intelligence is an additional weapon in the investor's arsenal. Fundamental questions to consider in this analysis include: Are competitors able to sell their services and products at abnormally low prices? If yes, is there a legitimate reason or is the real explanation that fraudulent methods are being employed, such as the use of substandard or counterfeit materials and products? Is there a cartel or similar organization in place that is preventing other companies from entering the market in general or a particular bidding process? Is it possible other relationships exist between competitors that would constitute unfair competition?

Safeguards against possible fraud and exposure to corruption during the project's execution are equally important. It is essential that corporate executives be aware of local and international laws, regulations, and industry standards, particularly when doing business in new jurisdictions. These must therefore be researched and resultant actions

and policies clearly communicated and enforced through appropriate training and periodic monitoring of the work underway. Additionally audits of, for example, purchase orders, invoices and payroll information will provide information that can raise red flags.

Brazil's need for transportation infrastructure is great, and the government's commitment to investment and to the industry is clear. Those wishing to take advantage of this tremendous opportunity, however, need to put in place protection against high levels of fraud.



**Vander Giordano** is a managing director based in Kroll's São Paulo office and specializes in business development for Latin America. He is a member of the Brazilian and International Bar Associations. Vander has extensive experience working with companies in the energy, retail, banking and airline industries.

**Allie Nichols** is a compliance associate based in Kroll's New York office. She is an attorney with business experience in Brazil and has published several articles in leading Brazilian publications.

**ECONOMIST INTELLIGENCE UNIT REPORT CARD**

**CONSTRUCTION, ENGINEERING & INFRASTRUCTURE**

The prolonged financial troubles of the construction sector, at least in developed markets, seem to have had a persisting moderating effect on fraud levels. Overall, the total number of companies hit by fraud dropped to 84%, and those that lost physical assets declined to 26%. On the other hand, management conflict of interest grew more common (28%) – the largest figure for any of the sectors surveyed. In fact, the overall picture is one of stasis. The construction sector now has the biggest problem with corruption (18%) compared with other sectors. On the positive side, construction companies are not waiting for an upturn to combat fraud. The survey shows them as the most likely to plan investment in six of the 10 fraud strategies covered, and the second most likely for the other four.

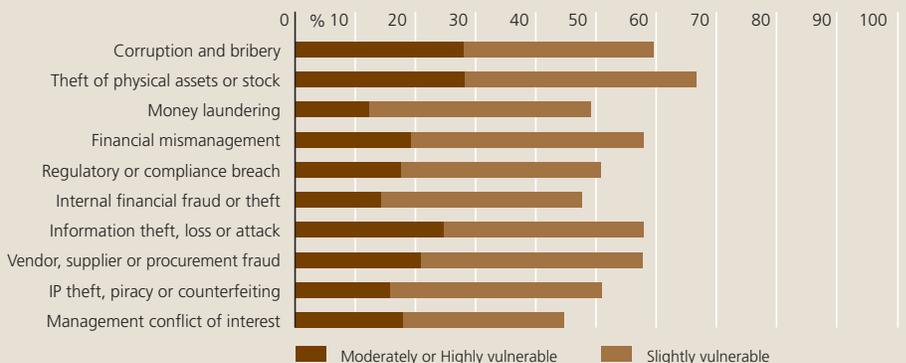
**Prevalence:** Companies affected by fraud 84%

**Areas of Frequent Loss:** Percentage of firms reporting loss to this type of fraud  
 Management conflict of interest (28%) • Theft of physical assets or stock (26%)  
 Information theft, loss or attack (21%) • Corruption and bribery (18%) • Vendor, supplier or procurement fraud (16%)

**Investment Focus:** Percentage of firms investing in prevention of this type of fraud;  
 Staff screening (65%) • Financial controls (65%) • Staff training (61%) • IT security (60%)  
 Management controls (56%) • Physical asset security (56%) • Reputation monitoring (54%) • Due diligence (53%)  
 IP and trademark monitoring program (53%) • Risk management systems (51%)

**Increase in Exposure:** Companies where exposure to fraud has increased 79%

**Biggest Drivers of Increased Exposure:** Most widespread factor leading to greater fraud exposure and percentage of firms affected; High staff turnover (35%)



# BRAZIL OVERVIEW



**Without a doubt, Brazil has a serious fraud problem. The incidence of all eleven types of fraud covered in the survey is higher in Brazil than the overall survey averages, and for eight of these crimes it is higher than the Latin American regional average.**

	2010	2009
<b>Prevalence:</b> Companies affected by fraud	90%	92%
<b>Areas of Frequent Loss:</b> Percentage of firms reporting loss to this type of fraud	Information theft, loss or attack (43%) Theft of physical assets or stock (30%) Management conflict of interest (30%) Vendor, supplier or procurement fraud (27%) Regulatory or compliance fraud (20%) Money laundering (17%)	Theft of physical assets or stock (33%) Management conflict of interest (33%) Internal financial fraud or theft (25%) Regulatory or compliance fraud (21%) Vendor, supplier or procurement fraud (17%) Information theft, loss or attack (17%) Corruption and bribery (17%)
<b>Investment Focus:</b> Percentage of firms investing in prevention of this type of fraud	Financial controls (60%) Physical asset security (53%) IT security (47%) Staff training (43%)	IT security (63%) Financial controls (54%) Management controls (54%) Staff training (50%) Staff screening (46%) Reputation monitoring (46%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	83%	79%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	IT complexity (43%)	IT complexity (50%)

More alarming still, Brazil surpasses the survey average in all regions for three types of fraud: information theft (43%), vendor or procurement fraud (27%), and money laundering (17%). Of note, the incidence of these particular frauds has become significantly more widespread. Over the past year, information theft more than doubled while money laundering more than tripled.

If anything, Brazilian companies do not seem to appreciate the extent of the problem. Typically, the number of respondents who report that they are either highly or moderately vulnerable to most frauds is roughly the same as the survey averages and for information theft it is even less (33% to 38%).

More important, Brazilian companies are much less likely than average to fight fraud actively. Every anti-fraud strategy listed in the survey sees significantly lower use in the country than for the survey overall. In eight out of 10 cases, the gap between the survey average for deployment and the Brazilian figure is greater than 10%. With only two exceptions – financial controls and physical asset security – anti-fraud investment in the coming year will also be below average. And, despite the pressing need, Brazilian firms are less likely than others to invest in IT security with fewer of them doing so than did last year.

Brazilian firms need to appreciate how big of a problem they have, and consider appropriate measures against it.

# Battling corruption and fraud in Colombia



By Andrés Otero & Ernesto Carrasco

Over the past eight years under President Álvaro Uribe, Colombia made dramatic strides in improving security and boosting investor confidence, advances that are applauded at home and abroad. Still pending, however, is a clear and energetic campaign to root out corruption. In the recent presidential election, won by Juan Manuel Santos, Uribe's former defense and economy minister, voters across the country expressed a clear desire for a robust rule of law and an end to crime and corruption. Similarly, while Colombia has increased the level of confidence in its legal system, according to *Doing Business 2009* – the annual country scorecard produced by the International Finance Corporation – it still has a long way to go in battling corruption, promoting transparency, enhancing the credibility of its courts, and, most importantly, resolving conflicts by institutional means rather resorting to the many forms of violence that have plagued the republic throughout its 200 year history.

Corruption and fraud in Colombia are not only real problems, but also problems of perception. Public opinion is often more easily outraged by a scandal involving a government minister, or by a high-level private sector executive, than by the constant bleeding of public health funds or by the kickbacks involving mid-level bureaucrats throughout the country. Both situations require urgent attention and decisive responses. While Colombia may have improved its ranking in Transparency

International's global Corruption Perception Index, the enduring perception among Colombians is that things have gotten worse. Most believe that the major infrastructure projects needed to help Colombia compete internationally are never completed or, at best, are finished after interminable delays because public servants and their private sector accomplices misappropriate the funds.

This perception of the situation, which to a large extent is correct, should signal to the new government the importance of implementing a coherent, sustained strategy to root out corruption, both public and private, which is clearly an obstacle to economic development. Clear and achievable goals are needed with the understanding that fraud and corruption can never be entirely eradicated. Only by doing so – and increasing the efficiency of, and return on, state-run investments – can Colombia, or any other emerging economy, improve its competitive position in the global marketplace. By leveraging the public's outrage, the Colombian government has an opportunity to change the country's "anything goes" culture and attack the scourge of corruption with a new sense of purpose.

In order to attack the problem effectively, though, it is essential to recognize that corruption is not confined to the government and to public contracts. It is just as common in the private sector and among non-governmental organizations. Whether we're talking about delivering humanitarian aid to Haiti or running the treasury operation of a privately owned bank, the risk of fraud or corruption is prevalent. In the latest annual

Global Fraud Survey, produced by the Economist Intelligence Unit for Kroll, Colombian business executives expressed great concern about fraud. The numbers are striking: 94% of those surveyed said that their company or organization had been the victim of fraud; 88% that they feel more exposed to the risk of fraud; and 97% that they were planning to invest in at least one new measure in the coming year in order to reduce the risk of their companies losing money through fraud.

The last of these statistics comes as no surprise. In the four years since opening the Kroll Colombia office, we have come to know a number of business executives who are conscious of the need to implement measures to counter operational risks in their companies. This is reflected in a significant growth of our fraud prevention services, a welcome but atypical situation. In many of the countries in which Kroll operates around the world, clients typically seek our services to investigate fraud or corruption when the deed has already been done. In contrast, Colombian business owners and executives are realizing that it is far more economical to invest in preventative measures than to react after the fraudsters have transferred stolen funds offshore or have themselves moved to other countries to enjoy their spoils.

Such investment is necessary because the traditional compliance culture that prevails today in most companies, as well as the regular internal audits and other controls, are often insufficient to detect and prevent fraud. Normal internal audit programs need to be complemented by methodologies that are based on experience gained from actual multidisciplinary fraud investigations. The objective is to prevent fraud from occurring and to identify new methods for combating this cancer.

Kroll Colombia has developed a methodology that helps reduce the number of frauds, in part by changing the culture within institutions. This methodology, which we call institutional integrity, begins with an analysis of standards and policies that already exist within a company, such as codes of ethics, corporate mission statements, policies and procedures for internal controls, audit reports, board directives, and various other manuals and guides. The goal is to transform all of these initiatives and controls into something more than a compendium of good intentions.

Integrity programs differ from industry to industry and from institution to institution,

but to succeed any such initiative must be set up with complete support and leadership from the top. It must also include tools for identifying risk, detecting different kinds of fraud, reporting irregularities, investigating when alarms are sounded, denouncing fraudsters to the proper authorities, and communicating to stakeholders. In addition, an integrity program must be adaptable, so that lessons learned from experience can be used to strengthen it further.

Ultimately, though, the goal is not simply to put in place good processes, however important they may be. Whether it is developing new rules for public bidding on government contracts, designing corporate responsibility guidelines consistent with both CSR best practice and the requirements of corruption regulation such as the FCPA and UK Bribery Act, conducting a due diligence investigation of a new hire, setting up a system of background checks on suppliers, partners, clients, and employees, establishing an integrity hotline to allow employees to report irregularities anonymously, or performing a fraud stress test in a company's treasury department, real change can only be accomplished through a shift in mentality and a policy of zero tolerance for fraud or corruption.

Very much contrary to the cynics who still maintain that the world is divided between those who have been caught and those who have not, Kroll is confident that a new class of business and political leaders is emerging. These individuals are guided by the conviction that doing the right thing and playing by the rules not only brings personal satisfaction but also pays big dividends for a company, an organization, or a country. Expectations in Colombia are high. Even so, we are optimistic that the country – including its politicians, business leaders, and ordinary citizens – can begin to position itself as an example to the rest of Latin America by proving that a country can grow and generate new opportunities by confronting corruption head on.

**Andrés Otero** is a managing director and head of Kroll's Miami office. He is an expert in a variety of investigative and intelligence areas, including fraud and anti-corruption services, dispute advisory and conflict resolution.

**Ernesto Carrasco** is an associate managing director and head of Kroll's Bogota office. He specializes in investigations into corporate and financial fraud for clients in Colombia, Panama and Chile.

## COLOMBIA OVERVIEW

The fraud picture in Colombia reflects in several ways an earlier level of economic development than that in many other surveyed areas. Companies, for example, are usually smaller ones: 94% had revenues of less than \$1 billion per year and 73% of less than \$500 million, compared to 66% and 49% respectively for the whole survey. Smaller businesses typically experience less fraud, and this holds true in Colombia to an extent: the incidence figures for most frauds are lower than average, in particular for theft of physical assets which affected just 12% of companies in the last year.

Digging deeper, however, reveals a serious problem that could get worse. Despite the advantage of smaller average size, 94% of Colombian businesses suffered some fraud in the last year, compared to 88% globally. Moreover, 88% of the country's respondents have seen their exposure increase, which is well above the survey average of 73%. Fraud is also stopping businesses from expanding: 52% of Colombian executives say their companies have been dissuaded from operating further in Latin America itself because of fraud.

At the moment, the biggest concern is vendor or procurement fraud: 24% of companies in the country experienced it in the last twelve months, against just 15% for the survey as a whole. Similarly, where respondents could identify who had committed a fraud in the last year, 21% of the time a vendor was the key perpetrator, a figure three times higher than the survey average.

The problems are likely to spread: 21% of companies reported IT theft or attack in this survey, and 42% that high staff turnover has increased their exposure, bringing the specter of a greater number of internal frauds.

Firms are currently ill-prepared to face this threat. Adoption of every anti-fraud strategy covered in the survey is significantly less widespread in the country than usual: for eight out of 10 strategies, Colombians are less than half as likely as the average to have invested in such protection. The one bright spot is that local businesses are scrambling to catch up. Planned investment for the next 12 months in these same strategies is 25% to 40% higher than in the rest of the world. Given the circumstances, this looks prudent.

	2009-2010*
<b>Prevalence:</b> Companies affected by fraud	94%
<b>Areas of Frequent Loss:</b> Percentage of firms reporting loss to this type of fraud	Vendor, supplier or procurement fraud (24%) Information theft, loss or attack (21%) Management conflict of interest (18%) Regulatory or compliance fraud (15%)
<b>Investment Focus:</b> Percentage of firms investing in prevention of this type of fraud	IP and trademark monitoring program (91%) Reputation monitoring (85%) Staff training (82%) Risk management systems (76%) Financial controls (73%) IT security (73%) Management controls (73%) Staff screening (73%) Physical asset security (70%) Due diligence (70%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	88%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	High staff turnover (42%)

\*Insufficient respondents in 2009 to provide comparative data.



# Risk governance for mines in emerging markets: **THE POWER BOTTLENECK**

By David A. Robillard

For centuries, mining companies have looked for ore throughout the world. Over the past decade, Chinese demand for natural resources and an increasing openness to foreign investment throughout Africa, Asia, and Latin America has increased the interest of this sector in emerging markets.

As a result, demand for skilled management has grown steadily for both in-country and head office positions. Many companies, however, struggle to find internationally experienced personnel to fill key positions, meaning that often senior managers do not understand the local culture or even the language. This can lead to overdependence on local managers, which greatly increases the risk of fraud.

The central problem with such situations is that they create an “obligation to trust” key local executives. Oversight is weakened as companies are unable to contradict a local manager on issues of fact or to present alternative interpretations. These managers in effect obtain a monopoly on information, which they can use to create a power bottleneck leaving them in almost complete control of the local operation.

Robert Kiltgaard has written extensively<sup>1</sup> on how such privileged positions enable corruption. His formula (Corruption = Monopoly + Discretion – Transparency) perfectly describes a situation where a senior executive controls the flow of information and in practice can be held accountable only with great difficulty.

Within the mining sector, many of these problems are often masked by external factors. Rising commodity prices, for example, may tempt head office to ignore autocratic managers who achieve good financial results over the short-term. Similarly, crises arising from community or governmental interference may further empower such managers.

Unless such bottlenecks are addressed, however, companies may find just about any type of fraud, from Foreign Corrupt Practices Act violations to sweetheart deals for family and friends, coming to light, usually at the worst possible time. Companies therefore need to be aware of signs of trouble:

- Those who exploit power bottlenecks often manage downwards through fear, forcing local personnel to show loyalty to “the boss” rather than to the company. These managers may even stoke up nationalistic fervor against foreign corporate owners.
- Such managers also resist providing timely and accurate information from local operations and restrict access of head office corporate officers to local community and government leaders as well as to key suppliers.
- The rotation of administrative staff tends to be frequent since those exploiting power bottlenecks do not tolerate dissent. Circumstances for staff departures tend to be unusual.
- Another red flag is atypical contract terms for employees and suppliers. Unusual contractual penalties to the company and prices out of sync with the market are particular favorites.

<sup>1</sup> Global Anti-Corruption Efforts: The Role of Non-Governmental Organizations”. Programme on Global Issues & Civil Society, Centre for Applied Studies in International Negotiations, 2007



**David A. Robillard** is a managing director based in Kroll’s Mexico City office. For more than 15 years, he has advised boards of directors and senior managers on matters of business partnering, corporate investigations and competitive risks in a range of industries, including mining, infrastructure and manufacturing.

## Important steps which can prevent trouble



- In assembling a management team, mining companies should consider both local and corporate needs. Language and cultural skills for managers who oversee operations are essential to counterbalance local management.
- Before hiring senior managers, an independent background investigation to uncover any hidden problems with a candidate’s professional or personal history is essential best practice. It is even more important when entering a new country or region.
- If the future of the company lies in emerging markets, consider rounding out board skills with local candidates who may come from within or outside the mining sector.
- Some companies form a local Board of Advisors to provide headquarters with advice and insight on local conditions or to be, during a crisis, a sort of “war cabinet.” Such a board should report to the corporate CEO and might include external counsel, government and community relations experts, communications and risk advisors, as well as others with useful skills and experience.

In searching for opportunities, companies cannot simply set up local operations that someone can exploit as their own fiefdom. Best practice needs to be as global as the opportunities businesses are chasing.

### ECONOMIST INTELLIGENCE UNIT REPORT CARD

### NATURAL RESOURCES

The natural resources sector has seen a shift in the types of fraud it faced. Theft of assets (28%), corruption (13%), and internal financial fraud all saw declines, while information theft (22%) rose and financial mismanagement (17%) as well as regulatory breaches (13%) both nearly doubled. The major issue looking ahead, however, is increased exposure: 80% of natural resources companies report that their exposure to fraud has increased, the second-highest figure in the sectors surveyed. Moreover, they are the most likely to face greater risk arising from increased collaboration (30%) and the second most likely for entry into new markets (27%). Greater investment in due diligence would be a natural response, but this is not the case in practice. Only 30% of sector companies plan to spend in this way in the next 12 months, compared to 41%, on average, across the other sectors surveyed.

**Prevalence:** Companies affected by fraud 91%

**Areas of Frequent Loss:** Percentage of firms reporting loss to this type of fraud

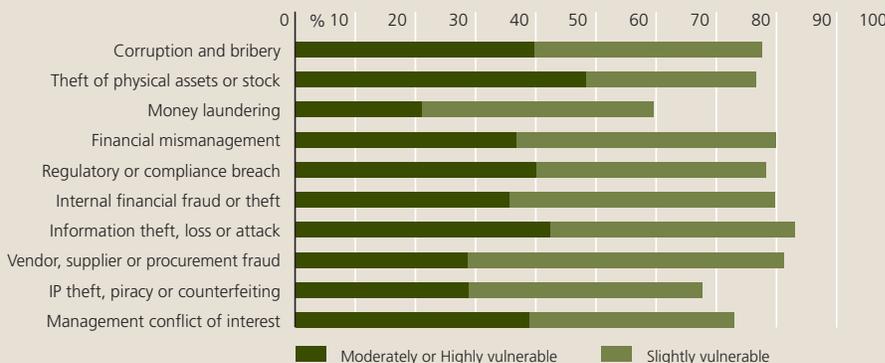
Theft of physical assets or stock (28%) • Management conflict of interest (27%) • Information theft, loss or attack (22%) • Vendor, supplier or procurement fraud (20%) • Financial mismanagement (17%)

**Investment Focus:** Percentage of firms investing in prevention of this type of fraud;

Financial controls (48%) • Physical asset security (43%) • Staff training (40%)

**Increase in Exposure:** Companies where exposure to fraud has increased 80%

**Biggest Drivers of Increased Exposure:** Most widespread factor leading to greater fraud exposure and percentage of firms affected; Increased collaboration with other firms (30%)



# ASIA-PACIFIC OVERVIEW

Asia-Pacific has the highest number of companies reporting being hit by at least one fraud in the last year of any region (92%), and it has an above average incidence for nine of the 11 frauds tracked in the survey.

In particular, in the last twelve months, Asia-Pacific companies had the most widespread problem with IP theft (16%) and money laundering (9%) of any region. Although its incidence of information theft (22%) was only slightly higher than last year and below the survey average, there are troubling signs in this area as well: respondents reported that 22% of all frauds in the last twelve months involved increased use of technology – the highest figure for any region. Anonymous emails were also involved in 23% of frauds, another regional high.

Asia-Pacific's poor fraud record is causing a correspondingly large concern among executives. The proportion of companies that see themselves as vulnerable to every fraud in the survey, as well as those planning to invest in each anti-fraud strategy covered is never far from the global average. More worrying is how many companies are looking to cut costs by weakening controls: 33% of firms reported that this practice had increased fraud exposure, up from just 19% last year. Add to this the continuing problems that Asia-Pacific companies have with high staff turnover, and there is no reason to expect a rapid change in the region's fraud numbers.

	2010	2009
<b>Prevalence:</b> Companies affected by fraud	92%	82%
<b>Areas of Frequent Loss:</b> Percentage of firms reporting loss to this type of fraud	Theft of physical assets or stock (28%) Management conflict of interest (25%) Information theft, loss or attack (22%) Vendor, supplier or procurement fraud (16%) IP theft, piracy, or counterfeiting (16%) Regulatory or compliance fraud (16%)	Regulatory or compliance fraud (27%) Information theft, loss or attack (19%) Vendor, supplier or procurement fraud (17%) Internal financial fraud or theft (16%) Management conflict of interest (15%)
<b>Investment Focus:</b> Percentage of firms investing in prevention of this type of fraud	Staff training (46%) IT security (43%) Management controls (42%) Risk management systems (42%) Reputation monitoring (41%) Financial controls (41%) Staff screening (40%) Due diligence (40%)	IT security (59%) Financial controls (52%) Physical asset security (46%) Management controls (42%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	75%	79%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	High staff turnover (34%)	IT complexity (35%)



# Fraud in India's manufacturing and engineering sector

By Richard Dailly

**India's economy is expected to expand by 8.5% this year and some estimate that growth may exceed 10% within the next few years. India's legal system, its use of English as the language of business, and a business culture already used to globalized markets, suggest that India's success story is likely to continue in the near future. This success arises at least in part from its domestic manufacturing and engineering sector. Centered in Chennai, Pune, and Kanpur, the sector contributes close to \$120 billion to GDP.**

Three key drivers are pushing its growth: the continued rise, importance, and economic might of India's middle class; foreign multinationals which have made India their manufacturing hub for global operations; and the continued need to develop India's infrastructure. The business opportunities are so large and the financial gains potentially so great that it is easy to overlook the potential fraud and corruption risks.

Fraud in India, however, continues to haunt business operations. According to the Global Fraud Survey, the top three frauds to which companies in India feel most vulnerable are:

- Information theft, loss, or attack (39% call their companies highly or moderately vulnerable);
- Regulatory or compliance breach (29%); and
- Intellectual property (IP) theft and counterfeiting (27%).

In Kroll's experience, the engineering, heavy engineering, and manufacturing sectors globally are often the ones most vulnerable to fraud and corruption. Thus, it is no surprise that the same survey indicates that the manufacturing sector faces a growing problem with vendor or procurement fraud and IP theft.

A key driver of fraud and corruption in the manufacturing and engineering sector is the frequently isolated geographical location of operations. While such a plant may manage itself on a day-to-day basis, in Kroll's experience its working methods and procedures are often open to abuse. Within an isolated plant, management is easily dominated by a key individual: checks and balances – the tools of accountability – can go out the window. When a powerful and charismatic individual manages an isolated

## POOR AWARENESS OF INTERNATIONAL ANTI-CORRUPTION LEGISLATION

Those companies in India that have a presence in the United Kingdom or the United States need to ensure they are not exposed unwittingly to the UK Bribery Act or the US Foreign Corrupt Practices Act respectively. Too few, though, are addressing bribery and corruption risks. As the latest results from the EIU's Global Fraud Survey highlight:

- Only 45% of respondents in India said their senior managers are thoroughly familiar with this legislation and a further 30% are unsure.
- Only 52% have in place a monitoring/reporting system to assess risks relating to the legislation on an ongoing basis.
- 55% say that they have adequate procedures to prevent bribery at all levels of operation, but 40% are uncertain.

facility with few accountability measures in place, the opportunities to manipulate tenders to friendly or related parties, to over invoice, and to pay kickbacks to business partners can be too tempting to resist. Consequently, procurement and contract fraud can be rife and also extremely hard to unearth.

As the survey also shows, an alarming 29% of fraud in India has as its key perpetrators vendors, suppliers, agents, and partners combined. Kroll has led several projects that investigated vendors and distributors of manufacturing or engineering companies. In this sector, such companies may be small partnerships, the details of which may not be recorded with the Ministry of Corporate Affairs. As a result, proving ownership can itself be problematic. Uncovering related party interests between distributors and contractors,

who may be old friends or family relations in a small and isolated community, almost always relies on intelligence because finding a paper trail will in most cases be impossible.

The questionable quality and trustworthiness of management running facilities can also heighten fraud risks. Often, a manager in such a plant has a technical background. He can solve problems at low cost, hire the most technologically sound research and development specialists, and suggest and implement unique engineering solutions. Despite these virtues, our experience tells us that such a pragmatist is also more likely to find solutions to problems which, while not malicious, may not be appropriate in the eyes of regulators. While it might be quicker, and part of the business culture, to pay local officials for a license to operate or to get distribution trucks across state borders, it does violate various local and international anti-bribery laws. What constitutes a facilitation payment can vary depending on the context, but unlike the US Foreign Corrupt Practices Act, which exempts ‘facilitating payments’ (defined as small amounts paid to governmental officials for the purpose of expediting fulfillment of a routine, non-discretionary duty), Indian law specifically forbids them.

Last but not least, because much of India’s heavy engineering growth is being driven by the race to improve local infrastructure, possible exposure to fraud exists when engaging with officials who might be involved in projects of national importance. The use of agents and intermediaries in India is common when dealing with government entities and often a conduit for a bribe. The potential sums involved in large infrastructure projects are huge. There is a real possibility of either knowingly or unknowingly wandering into an inappropriate transaction which, in a major infrastructure project, might have ramifications for years.

These are just a few ways in which the manufacturing and engineering sector faces unique and difficult fraud challenges in India. Kroll’s experience is that the three major problems highlighted – isolation, poor management, and a propensity for involvement in government contracts – often go hand in hand. It should be added that we have seen vastly different attitudes toward these issues. Operating on the ground, it is often obvious that management has to root out those who have taken advantage of their

positions in order to operate in their own interests. However, it is unfortunately not uncommon for the management of an entire facility to be implicated in wrongdoing.

Forewarned is forearmed: senior management at the head office must know how facilities are run and ensure that sufficient checks and balances are in place and that systems are fully accountable. With governments around the world stepping up efforts to fight corruption, not to know, or to turn a blind eye

to this crime could cost your company and its reputation considerable damage.



**Richard Dailly** is a managing director and head of Kroll’s operations in India. He has over 20 years of experience in global risk for the British government and Kroll. Richard has a deep understanding of investigative and intelligence gathering techniques, and assessment and analysis, in support of corporate investigations, political risk, litigation support, and multi-jurisdictional cases.

**Steps that Kroll has recently advised clients to take to minimize risk include:**

- Ensure that the corporate structure mandates accountability. Create structures which ensure that power does not lie with one individual answerable to nobody.
- Ensure that the culture is one of zero-tolerance to fraud and corruption. Training is essential at all levels. Ensure that the training is pitched correctly: junior employees need to understand and support good practice as much as senior management.
- A culture of transparency will deter fraud and corruption. Consider practices such as an “open-door” policy.
- Invest in a robust whistleblower system to help bring these issues to the attention of management in a timely and accurate manner.
- Do not leave facilities under the control of existing management without reviewing internal controls or introducing additional safeguards.
- Always question unusually large payments to agents, or a high number of payments to one particular agent.
- Always question a third party’s ongoing requests for cash payments – harder to establish a paper trail – or payment via offshore accounts.
- Always question the unnecessary use of third parties. Making payments to, or negotiating a contract through, multiple intermediaries is a cause for concern.
- Conduct thorough due diligence on agents and intermediaries prior to engaging them.

**ECONOMIST INTELLIGENCE UNIT REPORT CARD**

**MANUFACTURING**

The manufacturing sector presents a mixed fraud picture. On the positive side, the incidence of the majority of frauds covered in the survey declined, and the industry reported the lowest rates of information theft (13%), management conflict of interest (13%), and collusion (2%), when compared with other sectors. However, figures for specific regions – India or China, for example – may well paint a different picture.

Manufacturers face a growing vendor fraud problem (23%) – the second most widespread in the sectors surveyed. The incidence of IP theft also rose, to 11% from 7%. This is an above-average level and manufacturing companies are tied with healthcare ones as the most vulnerable to this crime (34% rank themselves as at least moderately vulnerable). Things could deteriorate, at least relative to other sectors. Despite the growing challenges, planned spending on IP protection and due diligence is less widespread than average.

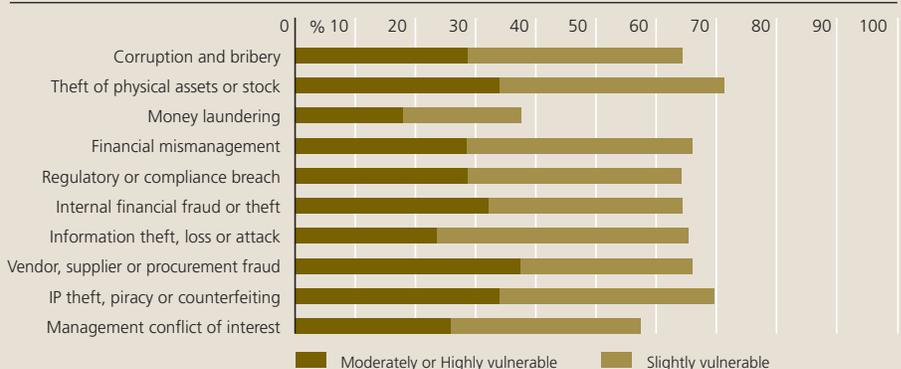
**Prevalence:** Companies affected by fraud 89%

**Areas of Frequent Loss:** Percentage of firms reporting loss to this type of fraud  
Theft of physical assets or stock (25%) • Vendor, supplier or procurement fraud (23%)

**Investment Focus:** Percentage of firms investing in prevention of this type of fraud  
IT security (43%) • Financial controls (41%)

**Increase in Exposure:** Companies where exposure to fraud has increased 68%

**Biggest Drivers of Increased Exposure:** Most widespread factor leading to greater fraud exposure and percentage of firms affected IT complexity (30%)



# CHINA OVERVIEW



	2010	2009
<b>Prevalence:</b> Companies affected by fraud	98%	89%
<b>Areas of Frequent Loss:</b> Percentage of firms reporting loss to this type of fraud	Management conflict of interest (30%) IP theft, piracy, or counterfeiting (26%) Theft of physical assets or stock (22%) Regulatory or compliance fraud (22%) Financial mismanagement (22%) Market collusion (22%) Corruption and bribery (20%) Vendor, supplier or procurement fraud (20%) Money laundering (20%) Information theft, loss or attack (16%)	Theft of physical assets or stock (31%) Internal financial fraud or theft (23%) Vendor, supplier or procurement fraud (23%) Information theft, loss or attack (23%) Management conflict of interest (19%) IP theft, piracy, or counterfeiting (19%) Regulatory or compliance fraud (19%) Corruption and bribery (15%)
<b>Investment Focus:</b> Percentage of firms investing in prevention of this type of fraud	IT security (56%) Staff training (54%) Financial controls (52%) Management controls (44%) Physical asset security (42%) IP and trademark monitoring program (42%) Staff screening (42%)	Financial controls (73%) IT security (54%) Management controls (46%) Physical asset security (42%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	72%	85%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	High staff turnover (34%) Weaker internal controls (34%)	IT complexity (42%)

Fraud in China is widespread and highly varied. Only 2% of respondents said that their company had not suffered any fraud in the past year. This incidence is up from last year but this may have as much to do with greater willingness to acknowledge fraud as with an actual increase.

No single type of fraud predominates. Instead, many are widespread: this year nine of the 11 frauds covered in the survey each affected at least one in five companies; last year seven of ten affected 19% or more. The incidence of individual types of fraud saw some notable shifts – the figure for management conflict of interest rose from 19% to 30% of companies, that for information theft dropped from 23% to 16% – but these are likely variations around a norm rather than signs of incipient trends. In fact, of the 11% who said that fraud had dissuaded them from operating in China – along with Africa, the most commonly cited region in the survey – information theft (named by 33% of this group) was the second most common specific issue, trailing only corruption (34%), and management conflict of interest was one of the lowest (10%).

Companies operating in China are starting to broaden their approach to fighting fraud. Last year's investment figures suggest perhaps an overreliance on financial controls. Although the number planning to invest further in these (52%) is still above the survey average, it is down from a year ago (73%). On the other hand, the number of those intending to put money into staff training (54%) and background checks (42%) has risen noticeably (from 35% and 31% respectively). This makes sense given that, according to Chinese respondents, the key perpetrator of fraud is an employee 42% of the time.

How effective these efforts will be, given the scale of the problem, is unclear. The number of companies that have partner, client, and vendor due diligence in place is well below the survey average (38% to 50%) as is the number intending to invest in this area in the coming year (32% to 41%), even though for 40% of frauds the main perpetrators in the last year were suppliers or vendors, and an additional 4% were customers. Worse still, 34% of respondents said that they had weakened their internal controls in the past 12 months, probably due to cost cutting. Given the fraud environment in China, many companies are going to have to do far more to protect themselves.



# Hand-in-hand: Corruption and private-sector fraud in China

Much like a ball of string, it can be hard to know where fraud begins and ends. A reluctance to discuss fraud has led many companies in China historically to hide behind questions of definition and underreport the problem. This year's Global Fraud Survey finding that 98% of respondents in the country suffered a fraud within the last year has one positive aspect: companies now at least acknowledge being victims. However, most respondents are not ready to admit that they could be hit again, still describing their companies as at most only "slightly vulnerable" to future attack.

By Violet Ho

Fraud and corruption are rampant and ongoing concerns in China. While both thrive on collusion, secrecy, and greed, corruption is a manifestation of fraud with the distinction that the people committing it occupy a public position – such as a civil servant or manager of a state-owned manufacturing plant. The combination of private sector fraud intertwining with public sector corruption can expose a company to compliance risk and sometimes prosecution under Chinese law. For a company operating in China's highly regulated industries, existing exposure to fraud is often exacerbated compared to other markets and can create the ideal environment for private sector fraud to mix with public sector corruption.

Kroll was engaged by one of the largest consumer goods importers in China after its Shanghai office was raided by customs officials. Financial documents and computers were confiscated and one of its senior executives detained. It later transpired that the executive in question had been bribing a number of customs officers so that they

would turn a blind eye to the false invoices that the company submitted to under-declare the value of the goods imported, and thus avoid import duties. The company was subjected to hefty fines and its business license was nearly revoked. Kroll's subsequent investigation revealed that the senior executive was also controlling a number of local distributors behind-the-scenes and was selling smuggled goods through the company's distribution network, leaving the client exposed to serious legal and financial damage.

It can be difficult to investigate fraud if only one or two people are involved but, like the case above, a single perpetrator will not be able to get very far without including others. Lone fraudsters will be motivated, often simply by greed, to recruit like-minded people in order to increase their potential financial reward and, as more people get involved, the scheme becomes more vulnerable to discovery. Often in China, the whistle is blown by one of the accomplices who is no longer happy with the financial reward that he or she is receiving.

Watching for certain warning signs can help detect this kind of situation or prevent it from happening. High staff turnover, especially among senior managers, should be a red flag. As corporate memory is lost, it becomes easier for corrupt staff to trick new hires into accepting a fraudulent status quo. An arrangement which makes corruption easier can be explained away as "the way things are done."

For foreign companies, a language and culture gap between senior management at home and local management in China can also be dangerous. So too can allowing a local CEO to become the single communication channel with headquarters. In China, senior hires commonly bring along a team from their former companies; this can result in cliques being formed that tie employee loyalty to the boss rather than the company.

### How to win the battle

This year's Global Fraud Survey found that China is the geographical area in which fraud has dissuaded the highest number of companies from operating, and that corruption was the primary reason. However, as Foreign Direct Investment figures show (see page 13), investment into China continues – and this is how it should be. Risk can and should be managed on a case-by-case basis.

There are steps companies can take to mitigate potential problems. When doing business in China, 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. It is no secret that the Chinese government plays a major role in all areas of business in China, and maintaining a good relationship with relevant government authorities is critical to the success of any enterprise. It is important to establish independently whether or not the local partner has the government relationships that he or she claims and whether this relationship is an institutional alliance based on operational strength and contributions to the local economy or, more dubiously, a relationship based on personal "blessings" from select individual benefactors.

In addition to the dual concerns of financial loss and violating Chinese laws, you may have exposure to extraterritorial regulation such as the US Foreign Corrupt Practice Act and the UK

Bribery Act. It is incredibly important in China, a jurisdiction with so much government involvement, to be able to demonstrate that you have taken all reasonable steps to know that your employees are not bribing officials.

Finally, if things do go wrong, get to the bottom of it by engaging professional help. Acknowledge the problem openly. Learn from your mistakes. And make sure it does not happen again.

As governments worldwide crack down harder on corruption – China itself is contemplating new legislation – the need for companies to put, and keep, their houses in order will only grow.



**Violet Ho** is a managing director and head of Kroll's operations in China. Violet has managed a wide range of risk consulting projects in Greater China ranging from fraud prevention to investigations of white-collar crime and distribution scams. She also manages investigative due diligence inquiries and assignments on business controls, intellectual property protection, employee risks, corporate security and crisis management.

### ECONOMIST INTELLIGENCE UNIT REPORT CARD

### CONSUMER GOODS

The consumer goods sector showed in the last 12 months that information theft and attack are not the only fraud issues. Although 25% of industry firms suffered from that crime – up from just 15% the year before – the proportion affected was still below the survey average (27%). Moreover, the sector had the lowest proportion of companies (18%) which blamed IT complexity for increasing their exposure to fraud – one of the few sectors where this decreased. The far bigger issue for consumer goods companies is that they have the most widespread fraud problem in the survey overall – 98% of firms were hit in some way. They were also the most affected by theft (43%) and financial mismanagement (21%) – the latter more than double last year's figure of 9%. Consumer goods companies also see themselves as more vulnerable than those in most other industries to corruption (45% highly or moderately vulnerable), theft (47%), and vendor or procurement fraud (36%).

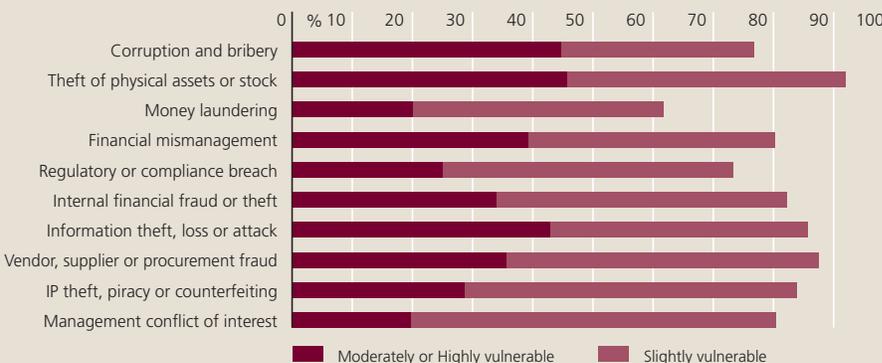
**Prevalence:** Companies affected by fraud 98%

**Areas of Frequent Loss:** Percentage of firms reporting loss to this type of fraud  
 Theft of physical assets or stock (43%) • Information theft, loss or attack (25%) • Financial mismanagement (21%)  
 Management conflict of interest (21%) • Vendor, supplier or procurement fraud (18%)  
 Internal financial fraud or theft (18%)

**Investment Focus:** Percentage of firms investing in prevention of this type of fraud  
 Physical asset security (64%) • IT security (59%) • Management controls (55%) • Staff screening (55%)  
 Reputation monitoring (55%) • Financial controls (54%) • Due diligence (54%)  
 IP and trademark monitoring program (48%) • Staff training (45%) • Risk management systems (45%)

**Increase in Exposure:** Companies where exposure to fraud has increased 61%

**Biggest Drivers of Increased Exposure:** Most widespread factor leading to greater fraud exposure and percentage of firms affected; High staff turnover (30%)





# Preventing the loss of trade secrets in China

By Tadashi Kageyama

Late on a Friday afternoon, the China CEO of a global specialty chemical products company receives a memo from its Head of Operations saying that a key engineer has tendered his resignation. This employee had been responsible for overseeing production of the company's soon to be launched, high-end product that is considered central to future growth. He is leaving, he says, to return to his home town in order to support his small, family-run business. It might sound straightforward, but it is far from it.

Within a month, more than twenty local staff members left. On one day alone, employees from research and development (R&D), procurement, production, quality control, and finance tendered their resignations. Senior management in China and at headquarters started to worry.

The company in this real case called in Kroll. We gathered intelligence from sources in the company's supply chain and forensically examined computers used by the former employees. After weeks of investigating, it became clear that these individuals had left in order to follow the chief engineer, who had actually moved to a local competitor.

Furthermore, the investigation uncovered evidence that some employees had stolen proprietary information including, but by no means limited to, designs, layout of the production facility, vendor lists, marketing plans, employee contact information, management reports, and financial information – what the client would rightly consider its trade secrets. Soon after the investigation, the local management team heard rumors that the competitor which had hired its old staff members would soon launch a high-end product very similar to the one the departed engineer had overseen.

Incidents like this occur frequently in emerging markets. Companies fail to secure trade secrets, making it all too easy for wrongdoers to steal and replicate key products in a matter of weeks. In this case, the company lost out on market share and potential revenue costing millions of dollars in forecast revenue. The results of the investigation were an eye opener for the client, and Kroll was further retained to conduct an audit of the client's entire local operations, from physical and technology security to operational and human resources security. We helped the client identify and resolve potential risks in order to avoid such a situation from reoccurring in the future.

Intellectual property (IP) and information theft are particularly common in the healthcare, pharmaceutical, and biotechnology sector in China. Local and international companies are shifting their operations in the country from low-end to high quality product manufacturing as well as from pure production to R&D facilities. This has driven growth in the chemical industry in China as well to annual levels of some 30%. As healthcare and chemical companies fight for market share and revenue, they sometimes resort to unethical means.

According to this year's Global Fraud Survey, IP theft is the second most common fraud in China, and is tied with information theft, loss, or attack as the most widespread in

the healthcare, pharmaceutical, and biotechnology sector.

Although, as in the above example, IP loss is often at the hands of employees, they are far from the only culprits. External parties may try to obtain information through hostile means such as hacking into computer networks or breaking into company premises. They might also be more devious, by setting up a fictitious company to impersonate a potential big buyer and by producing false information, only to lure victims into revealing valuable proprietary information. In one such case, we found that a competitor was bribing our client's employees and vendors to act as informants.

We have also seen cases where a client's customer passed on proprietary information to competitors. In fact, on one occasion, although anonymous whistleblower letters accused two senior employees of stealing the IP of their former employer (Company X) and using it to design and launch new products, our investigation uncovered that one of Company X's key customers in fact passed on this information to the accused employees and demanded that they make products at a lower cost.

Given the many possible ways that trade secrets can be compromised, it is critical to take a holistic perspective toward all threats, both internal and external, and to tailor security and controls accordingly.

The first step for companies protecting themselves in China, though, is to understand what constitutes their own IP. Although multinationals in Asia implement policies, procedures, contracts, and agreements to mitigate the loss of patents, designs, copyrights, and trademarks, they often neglect to put in place integrated solutions to protect their trade secrets. The World Intellectual Property Organization (WIPO) defines trade secrets as "any confidential business information which provides an enterprise a competitive edge". Such IP, also called "know-how", can be difficult to control since it is usually intangible and ingrained in people's minds. Making matters worse is that non-compete and non-solicitation agreements signed between companies and their employees – common tools to protect trade secrets – are difficult to enforce in Asia. Therefore, implementing robust controls and a response plan is extremely important to limit any potential damage.

Achieving a commercially reasonable level of security, though, is no easy task. The most effective solution will include physical security, information and computer security, operational security, human resource

security, and communication security. Of course, these categories not only overlap, but they are also constantly evolving. An effective solution must, therefore, encompass them all. Based on our experience around the world, the so-called "divide and conquer" approach to IP protection – trying to address, say, computer security without integration with areas such as human resource or physical security – simply does not work. Add to this the unique challenges relating to chemical and biotechnology R&D and production facilities, as well as understanding the laws and regulations of each country where IP is to be stored or sent, and the extent of the task starts to become clear.

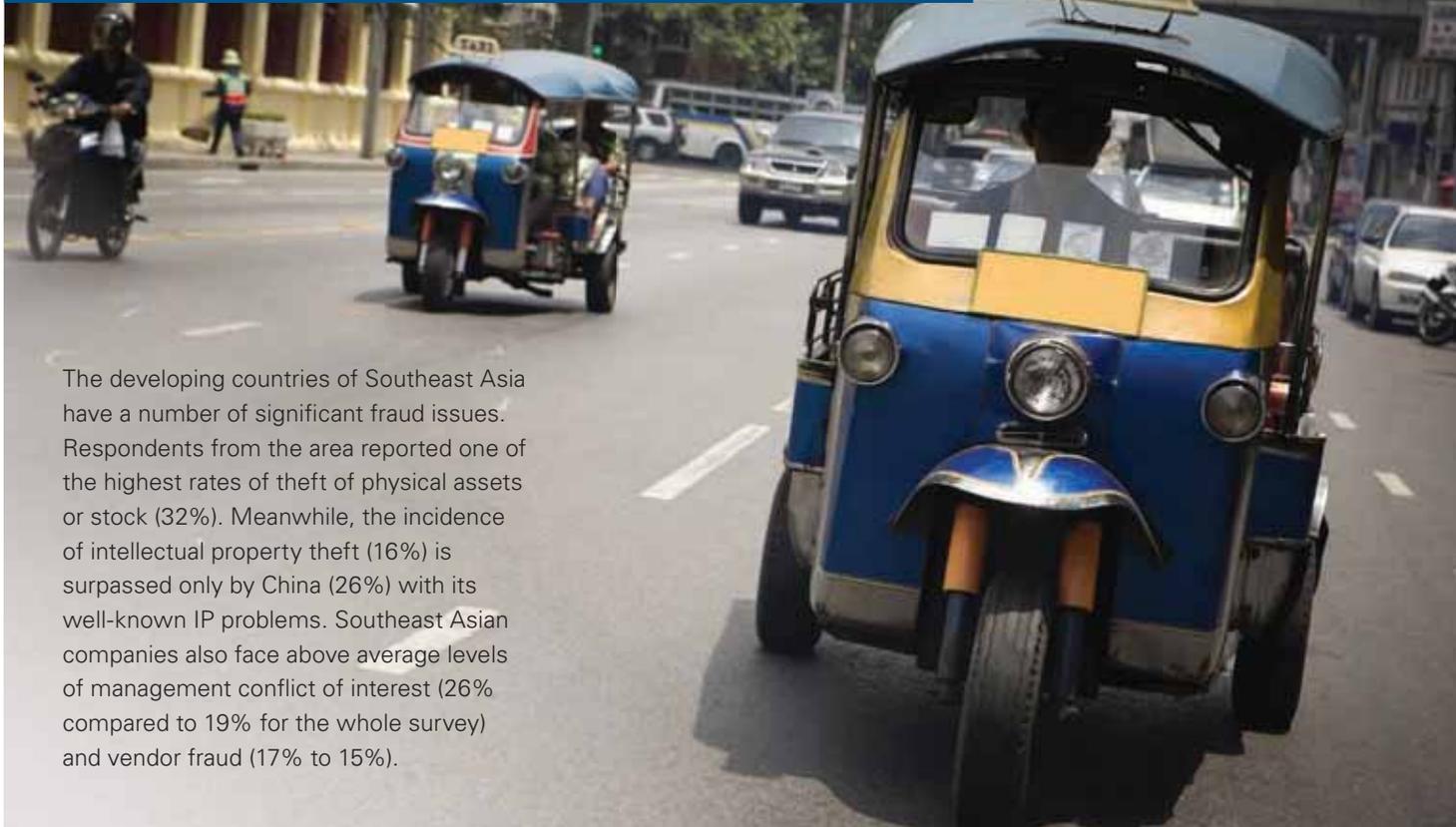
The best place to begin is a risk assessment, in order to look for any risk factors which can be quickly and cost-effectively mitigated – useful easy wins – and any issues that may require longer term solutions. Typically, such an assessment starts with a thorough review of the current operational and technology environments along with the current state of IP protection. It is also important not to assume that policy is the same as reality. Identifying – through document analysis, interviews, sample analysis, or covert and unscheduled visits – areas where plans and policies are not actually being followed is essential. In a recent case, company policy required highly secure and centrally managed wireless data networks. Our on-site testing found, however, that completely unsecured wireless networks were in use, were undocumented, and were placing IP at serious risk.

Completely eliminating competitors from trying to compromise trade secrets is not a realistic goal. Neither is trying to prevent an employee from moving to a competitor or setting up a competing business. Companies can, however, do more to mitigate the risk of loss or theft by re-evaluating and understanding what IP they have that goes beyond patents and trademarks, and how these trade secrets are created, controlled, and destroyed. Conducting an audit of business operations and facilities is another useful step in identifying vulnerabilities and fraud entry points. Ultimately, though, integrated security arrangements need to treat trade secrets as the important pieces of IP that they are.



**Tadashi Kageyama** is a senior managing director specializing in business intelligence, investigations, and risk consulting services for corporate clients and government agencies. Prior to joining Kroll, he was a global purchasing agent for Mitsubishi Heavy Industries Ltd and worked as a staff writer for Nihon Keizai Shinbun (Nikkei).

# SOUTHEAST ASIA OVERVIEW



The developing countries of Southeast Asia have a number of significant fraud issues. Respondents from the area reported one of the highest rates of theft of physical assets or stock (32%). Meanwhile, the incidence of intellectual property theft (16%) is surpassed only by China (26%) with its well-known IP problems. Southeast Asian companies also face above average levels of management conflict of interest (26% compared to 19% for the whole survey) and vendor fraud (17% to 15%).

	2009-2010*
<b>Prevalence:</b> Companies affected by fraud	90%
<b>Areas of Frequent Loss:</b> Percentage of firms reporting loss to this type of fraud	Theft of physical assets or stock (32%) Management conflict of interest (26%) Information theft, loss or attack (25%) Vendor, supplier or procurement fraud (17%) IP theft (16%)
<b>Investment Focus:</b> Percentage of firms investing in prevention of this type of fraud	Management controls (53%) Due diligence (53%) Reputation monitoring (52%) Staff training (49%) Risk management systems (48%) IT security (47%) Staff screening (47%) Financial controls (46%) IP and trademark monitoring program (46%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	74%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	Weaker internal controls (35%)

\*Insufficient respondents in 2009 to provide comparative data.

Businesses in the region are aware that all is not well, but may not always focus on the correct problem. For eight out of the 10 frauds, Southeast Asian respondents are nearly twice as likely than average to identify themselves as highly vulnerable. Sixteen percent of Southeast Asian respondents feel highly vulnerable to the threat of corruption and bribery compared to the global average of 8%. For internal financial fraud or theft, 14% of respondents feel highly vulnerable to this risk compared to the global average of 5%.

Companies in the region are also more active than most on anti-fraud measures. Every strategy examined in the survey is more widely deployed than average except for financial controls (68%) and IT security measures (64%) where the difference from the global figure is just 1% in each case. Forty seven percent of companies currently invest in IP protection compared to the survey average of 38%. Forty six percent of companies in Southeast Asia plan to invest further in IP protection in the next 12 months – the survey average is just 37%.

Inconsistency, however, may end up hurting Southeast Asian companies. While more firms than average are making investments in anti-fraud measures, 35% are weakening controls in order to save money – the highest level for any region. Given the challenges that Southeast Asian companies face, it looks like trouble ahead.

Such a range of techniques and approaches is important when conducting investigations in Indonesia because the risk of corruption is not normally apparent and certainly cannot be detected through regular financial and legal due diligence. In such a market, where wealth is closely tied to sponsors or families, prior to entering into any definitive agreement it is absolutely critical to gain a comprehensive understanding of the business ethics and reputation of potential partners as well as their management style, backgrounds and political connections. One important issue to consider is the presence of any hidden ties to political or military interests, especially in Indonesia's resources, energy, and transportation sectors. Such connections can, at best, severely affect a company's operations under certain circumstances and, at worst, trigger significant liabilities for foreign partners under anti-corruption legislation back home, notably the US Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act.

Another significant issue to investigate is the possible existence of any undisclosed related-party transactions between the company being considered for an investment and the wider family interests of current owners. These are often used to channel funds from the company to other family businesses to the detriment of foreign investors. Kroll recently investigated and uncovered just such a scheme in Indonesia for a grateful financial investor.

The need for foreign investors – financial or strategic – to be vigilant does not end once the investment has been made. In a market where corruption appears institutionalized as an accepted business practice, the severe penalties and extraterritorial reach of legislation such as the FCPA and the UK Bribery Act make it imperative to conduct regular, ongoing “audits” of suppliers, customers, agents, distributors, and local management. After all, according to the Global Fraud Survey, approximately 47% of fraud in Southeast Asia markets is perpetrated by employees – and those are just the cases that come to light.



**Chris Leahy**, a managing director of Greater China and Southeast Asia, has extensive experience advising corporates, financial institutions and governments on matters relating to pre-transaction and post-transaction investigations, due diligence, regulatory compliance and corporate governance.

## Indonesia's darker side

By Chris Leahy

With GDP growth of 4.5% last year and a forecast increase of 6% for 2010, Indonesia has become one of Southeast Asia's most popular destinations for foreign capital. Particularly attractive for investors are the infrastructure, energy, and transportation sectors, where the government of President Susilo Bambang Yudhoyono acknowledges a chronic need for foreign money. Despite its bright investment prospects, however, Indonesia has a darker side: the endemic corruption that too often greets unsuspecting investors once deals have closed. Indeed, respondents to this year's Global Fraud Survey based in Southeast Asia, feel especially vulnerable to the risks of corruption, bribery, and regulatory breaches.

Kroll advises a significant number of clients on understanding and negotiating the risks inherent, although not always transparent, in any investment in Southeast Asia. We also assist clients when prior investments have not turned out as expected, often because of insufficient reputational due diligence before investing. Much of this post-transactional work takes place in Indonesia. For example, Kroll advised a foreign client caught in a legal and commercial dispute with its local partner in the country that revolved around disagreements over strategy and direction in several shared business ventures. The relationship had become so strained that the foreign party needed to exit and turned to us for help because it understood that, in Indonesia, a legal exit strategy alone was unlikely to resolve these issues. Kroll used various investigative techniques and lines of inquiry to obtain actionable intelligence and evidence that strengthened the client's hand in obtaining a commercial settlement between the two parties.

# EUROPE OVERVIEW

Compared to other regions, European companies did very well over the last year in the fight against fraud. The continent saw the lowest percentage of companies hit by at least one fraud (83%), a figure which was below last year's as well. Europe also had a below average incidence of every fraud covered in the survey, and the lowest of any region for four out of 10 – theft of physical assets (23%), information theft (19%), regulatory or compliance theft (6%), and money laundering (4%). Nearly half of European companies (47%) even reported that they had lost no money to fraud in the last year.

Responses were broadly consistent across Europe, though interestingly the UK recorded above average levels of both internal fraud and fraud committed by senior management.

The biggest danger amid such undeniable good news is taking one's eye off the ball. After all, the good performance is only relative: more than eight in 10 European companies were hit by a fraud in the last year. Furthermore, the number of companies seeing an increased fraud exposure (73%) is the same as the average.

Some signs suggest that European businesses might fall victim to complacency. They are already less likely than average to have adopted most anti-fraud strategies in the survey. For the only two exceptions, risk management systems (adopted by 51%) and reputation monitoring (50%), the difference between the European and the global figures is, in both cases, just 1%. Slightly more worrying, for eight out of 10 of these strategies, investment will be less widespread in Europe than globally, although admittedly the gap is usually small.

If European companies want to continue to lead on tackling fraud and to address the crime's continuing pervasiveness on the continent, they will have to push harder rather than rely on a relatively quiet environment.

	2010	2009
<b>Prevalence:</b> Companies affected by fraud	83%	89%
<b>Areas of Frequent Loss:</b> Percentage of firms reporting loss to this type of fraud	Theft of physical assets or stock (23%) Information theft, loss or attack (19%) Vendor, supplier or procurement fraud (14%)	Theft of physical assets or stock (32%) Management conflict of interest (25%) Regulatory or compliance fraud (19%) Information theft, loss or attack (17%)
<b>Investment Focus:</b> Percentage of firms investing in prevention of this type of fraud	IT security (51%) Staff training (42%) Management controls (41%) Staff screening (41%) Financial controls (41%) Due diligence (41%)	IT security (49%) Financial controls (45%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	73%	70%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	IT complexity (29%)	IT complexity (31%)

# Investigations and the use of technology

**Identity theft and internet frauds have been leading items on the media crime agenda over the past few years, but the use of technology in investigations remains, for most people, confined to TV police shows, where specialists use a wide array of highly sophisticated instruments in cutting edge laboratories to solve complex crimes. This is slightly misleading: technology can be user-friendly and is very widely deployed in all types of investigations.**

By Marianna Vintiadis

Litigation support is dominated by legal technologies. Such advanced electronic tools, the development of which is driven mainly by e-discovery needs and standards in the United States, allow specialists to search for, capture and recover relevant data. However, many applications, often freely available on the internet or found in software designed for office or home use – such as word processing packages – can be very useful tools in investigative work as long as their limitations are properly understood.

A prime example is the study of metadata – data stored within files containing information about the files themselves. A text document, for example, can have buried in it data about its author, its original file location and creation date. A typical area where such metadata can prove useful is the investigation of anonymous letters: a few simple steps taken on your home computer with software you use daily can sometimes reveal the identity of a poisoned pen.

Identifying who has registered the domain of a fraudulent website can also be very useful. Web addresses have to be registered and it is quite easy to identify the registrant's name by performing a simple check over the Internet, sometimes with surprising results.

It is not unknown for fraudsters to register domains in their own names. Similarly, information linking a site to the identity of its owner can be buried in the program instructions of the web page, also known as its source code. Most browsers allow users to examine source codes with two simple mouse clicks.

A slightly more sophisticated approach can be the use of a web crawler, or web spider, to analyze a website. This is a computer program that can index the information and links on a particular site. Navigating through an ill-structured site or one deliberately designed to be opaque can be very difficult. If instead all the information is crawled and then downloaded onto a computer, it can be indexed

and searched a lot more simply and efficiently. A typical use of a web crawler could be in investigations of corrupt tendering. Here too much information is often put online and made publicly available in order to hide a piece of key information while technically complying with formal advertisement requirements.

Do the above examples mean we can all be e-detectives? It is not that simple: metadata can be manipulated; registrants can be as fake as the websites they register; and do-it-yourself home indexing and searching techniques can lead to partial results or to the production of overwhelming amounts of information that require specialist skills to process. Even worse, accessing an electronic document without using a forensically sound

technique can sometimes compromise its integrity and therefore its future use as evidence in court.

Knowing the limitations of your software or the technique you are using is part of the expertise required for a successful investigation. Experienced investigators need a range of techniques and technologies in the digital world but will also understand that the appropriate one can sometimes be very basic. Moreover, the traditional skills of the investigator in structuring an investigation and analyzing data are still of utmost importance. The tools may have changed but the investigative art remains fundamentally the same.



**Marianna Vintiadis** is Kroll country manager for Italy and Greece. A trained economist with experience in policy making and analysis, she works on business intelligence and complex investigations in these countries. Her areas of expertise include market entry, shipping, piercing the corporate veil, and internet investigations.

## ECONOMIST INTELLIGENCE UNIT REPORT CARD

## PROFESSIONAL SERVICES

Overall, the professional services sector is doing well at tackling fraud, compared to other industries, but this may be leading it to be complacent about its weaknesses. The industry has the lowest percentage of companies affected by fraud in the survey (81%), and also the lowest incidence of theft of physical assets (18%), vendor or supplier fraud (9%), and internal financial fraud (4%). Success, however, is relative: fraudsters took advantage of eight out of every 10 professional services firms in the last year alone. Moreover, the industry has the second-highest level of information theft (40%), and above-average incidences of corruption (13%) as well as IP theft (11%). Nevertheless, it will see the least widespread investment in IT security (37% – or fewer than those who experience IT fraud), risk systems (30%), and IP protection (25%).

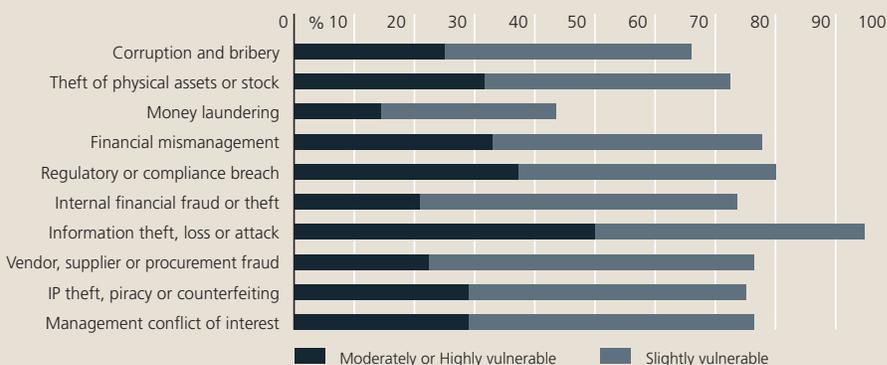
**Prevalence:** Companies affected by fraud: 81%

**Areas of Frequent Loss:** Percentage of firms reporting loss to this type of fraud: Information theft, loss or attack (40%) • Theft of physical assets or stock (18%) • Management conflict of interest (16%)

**Investment Focus:** Percentage of firms investing in prevention of this type of fraud: Management controls (41%) • Reputation monitoring (40%)

**Increase in Exposure:** Companies where exposure to fraud has increased: 70%

**Biggest Drivers of Increased Exposure:** Most widespread factor leading to greater fraud exposure and percentage of firms affected: IT complexity (28%) • High staff turnover (28%)





# FRAUD IN THE GULF: For better or for worse?

By Tom Everett-Heath

The economic turmoil in the Gulf over the last two years has made several things clear: the region is now inextricably woven into the global economic and financial systems; despite continued dependence on hydrocarbons, demographic changes have made necessary radical structural adjustment of regional economies, a key part of which is massive infrastructure investment; the quality of corporate governance has not grown as rapidly as the regional footprints of international corporations or the balance sheets of regional businesses; and the regional response to white-collar crime has shifted from denial to action.

Underpinning all of this is the reality that the Gulf remains in transition. Prior to the global economic crisis, it saw years of double digit economic growth, with domestic private and public sector entities leaving plenty of room at the trough for international business. More recently, famine has followed feast in some markets: Dubai is an obvious geographic example; real estate a sectoral one; and equity capital markets a structural one. However, elsewhere, despite bumps on the road, the direction of travel remains unaltered.

The liquidity crunch did jolt the region's business culture. Several large-scale frauds have been exposed involving sovereign wealth funds, government-owned entities, and private sector businesses. Some have

been reported and publicly scrutinized, such as the Deyaar and Damac scandals in Dubai and the Saad-Al-Gosaibi case; many others have not.

Whether the incidence of fraud is, in absolute terms, rising in the Gulf, or greater awareness and intolerance of it have created that impression, is open to debate. The Global Fraud Survey indicates significant worry about its spread: 40% of Middle Eastern respondents said that fraud had grown worse at their companies in the last year – the highest figure for any region. Kroll's experience suggests that the speed of economic growth during the boom, particularly from 2005 through 2008, and the concomitant stretching of oversight,

compliance, and the capacity to manage counterparty risk, led to increased levels of fraud. Only recently, however, has evidence of these crimes begun to emerge in the public domain.

The key change, though, has not been statistical. It has been in the attitudes of the regional elites – political, business, and regulatory – to fraud. In the past, those with power went to great lengths to keep such issues behind closed doors, or at most to deal with them discreetly in the diwan and majlis. Now, there is an appetite to investigate and to pursue assets across borders and through the courts. Regional governments and private sector entities have engaged Kroll to investigate a growing number of these frauds over the last few years, and we have seen an increased cultural acceptance in the region that consultants and lawyers have a role to play in such activities.

For those considering fraud investigations in the Gulf, the basics apply here as much as anywhere: act early; be decisive and thorough; secure data and other evidence; be aware of chain of custody issues; understand the local context and the vested interests involved when formulating strategy, as there may be more stakeholders than you realize; think hard about the jurisdictions in which you take action, how the relevant authorities can best help you, and how they might be encouraged to do so.

Of course, prevention is better than cure. For international businesses active in the Gulf, the most important way to reduce the risk of fraud is to develop a robust understanding of local partners – be they domestic management, owners of counterparties, co-investors, customers, clients, suppliers, contractors, sales agents, overseas representatives, fiduciary agents, etc. Going beyond publically available information and getting comfortable with the seven “C” risks – Commitment, Capability, Capacity, Collection, Contract, Credibility, Corruption – will go a long way toward protecting business integrity.



**Tom Everett-Heath** is a managing director and the head of Kroll's Middle East business. He works with clients on identifying, understanding and managing risks involved in mergers and acquisitions, corporate finance transactions and new market entry.

Tom specializes in supporting clients' management of disputes, asset recoveries, counterparty exposure, reputational liabilities, political risk, capital market opportunities and internal fraud reviews.

## MIDDLE EAST OVERVIEW

At first glance, the Global Fraud Survey figures for the Middle East suggest that the region is not doing badly compared to other parts of the world. The overall incidence is the same as the global average. Although companies in the region face significant problems with information theft and physical theft, so does everyone else and the Middle East's figures are only slightly above normal. The region's incidences of seven of the eleven frauds covered in the survey are below average, and for three – management conflict of interest (12%), vendor fraud (9%), and IP theft (2%) – the Middle East has the lowest rate of any region.

Digging deeper, however, the picture is not so positive. To begin with, respondents from the Middle East come from the smallest companies on average of any region: 81% have annual revenues of less than \$1 billion, against 66% for the survey as a whole. As smaller companies tend to have lower rates of fraud, this goes some way toward explaining the region's apparently positive picture. Other data points in the opposite direction: 45% of all companies had an

employee commit a fraud within the last year, meaning that employees made up 61% of known perpetrators, in both cases the highest figures for any region. The Middle East also had the second highest figure – after Africa – for companies suffering at least some financial loss (70%).

The bigger concern, though, is about the future. Forty percent of Middle Eastern respondents said that fraud had grown worse at their companies in the past year – the highest figure for any region – and for every fraud covered in the survey, the number who rank their businesses as at least moderately vulnerable is higher than the survey average. That goes a long way toward explaining the very high investment rates in anti-fraud strategies in the region (listed in the below chart).

Despite apparently having performed relatively well compared to the rest of the world, survey respondents in the Middle East understand that theirs is a region where fraud risks are higher than normal and it is necessary to protect companies accordingly.

	2009-2010*
<b>Prevalence:</b> Companies affected by fraud	86%
<b>Areas of Frequent Loss:</b> Percentage of firms reporting loss to this type of fraud	Information theft, loss or attack (30%) Theft of physical assets or stock (30%) Internal financial fraud or theft (21%) Financial mismanagement (19%)
<b>Investment Focus:</b> Percentage of firms investing in prevention of this type of fraud	IT security (70%) Financial controls (67%) Physical asset security (63%) Management controls (58%) Staff training (54%) Staff screening (51%) Risk management systems (51%) IP and trademark monitoring program (51%) Reputation monitoring (51%) Due diligence (42%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	70%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	IT complexity (35%) Entry into new, riskier markets (35%)

\*Insufficient respondents in 2009 to provide comparative data.

# AFRICA OVERVIEW

The proportion of African-based companies that reported being affected by at least one fraud (87%) is very slightly lower than the survey average (88%). That is about the only positive thing that can be said regarding the fraud picture in Africa. For eight of the eleven frauds covered in the survey – information theft or attack, theft of physical assets, management conflict of interest, financial mismanagement, internal financial fraud, vendor or procurement fraud, corruption, and market collusion – the continent had the highest incidence for any region. For regulatory or compliance fraud, it came a close second (20% to 21% in Latin America). Although a number of frauds were slightly less widespread this year than last, this decline was more than offset by large increases in others, notably management conflict of interest and information theft, where the incidence roughly doubled.

Fraud vulnerability data paints a similar picture. African respondents are more likely to consider themselves highly vulnerable and moderately vulnerable to every fraud in the survey, often by a very wide margin. For example, 22% say that they are highly vulnerable to corruption, compared to a

survey average of 8% – and corruption was one of the frauds that was slightly less widespread in this year's survey compared to the last one.

Companies in Africa do try to defend themselves. Every anti-fraud strategy in the survey is more widely adopted in Africa than on average except for IP protection, and IP theft is one of the few areas where the incidence of fraud on the continent is below average. In fact, five of these strategies are more commonly deployed in Africa than in any other region, and for three others Africa comes in second. The problem is, simply, that they do not appear to be working. There is little reason for hope going forward. The number of companies looking to invest further in anti-fraud strategies is in most cases only close to average and in some cases significantly below.

The survey also points to one of the ways in which widespread fraud is frustrating economic investment: it has dissuaded 11% of companies worldwide from operating in Africa, tying with China for the highest figure in this regard. China, however, can find other investors easily at the moment. Africa needs them rather more.

# Risk and reward: Fraud and the African telecoms industry

By Paul Adams

The Global Fraud Survey results depict a stark image of the risks of fraud in Africa. Add legitimate worries about political instability and the legal enforceability of contracts and licenses, and is it surprising that many companies are reluctant to enter this growing but difficult market? Yet investment decisions balance perceived risk and reward: a weak recovery in developed economies and rapid development of industry and services has increased the lure of Africa.

One sector that presents particular opportunities is telecommunications, as the rapid uptake of cell phones and broadband makes the African market one of the world's fastest growing. The rate of cell phone adoption, for example, is twice that of Asia, and in Nigeria subscriber numbers have soared in the last decade from a few thousand to 75 million with demand set to grow by 25% per year.

Factors which portend further growth in the telecoms sector include:

- The laying of sub-sea cables which will enable a steep rise in internet connections and use;
- Demand from an emerging middle class which craves internet access and a smart phone as status symbols;

	2010	2009
<b>Prevalence:</b> Companies affected by fraud	87%	89%
<b>Areas of Frequent Loss:</b> Percentage of firms reporting loss to this type of fraud	Information theft, loss or attack (41%) Theft of physical assets or stock (41%) Management conflict of interest (39%) Financial mismanagement (35%) Internal financial fraud or theft (30%) Vendor, supplier or procurement fraud (26%) Regulatory or compliance fraud (20%) Corruption and bribery (17%) Market collusion (15%)	Theft of physical assets or stock (43%) Internal financial fraud or theft (26%) Financial mismanagement (26%) Vendor, supplier or procurement fraud (22%) Corruption and bribery (22%) Management conflict of interest (20%) Regulatory or compliance fraud (20%) Information theft, loss or attack (20%)
<b>Investment Focus:</b> Percentage of firms investing in prevention of this type of fraud	IT security (50%) Staff training (44%) Risk management systems (44%)	Physical asset security (57%) IT security (56%) Financial controls (52%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	70%	83%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	IT complexity (39%)	High staff turnover (37%)

- The savings, increased disposable income and combined buying power of many millions of low-income Africans; and
- New technology making payment systems more available to the mass market.

All five top causes of fraud are a concern in the telecom sector, which faces a range of frauds – from simple theft, through to sophisticated call rerouting, to worrying degrees of possible regulatory exposure.

The problems with corruption, the leading issue for survey respondents, were demonstrated recently by questions surrounding the integrity of the bidding process for Nigeria Telecommunications Ltd and the price paid for state-owned Zamtel in Zambia. Nevertheless, African respondents to the survey were among the most confident from any region that they had the understanding and procedures needed to minimize breaches of the US Foreign Corrupt Practices Act and the UK Bribery Act. The number of major regulatory investigations into corruption by multinational companies' operations in Africa underlines the need for such awareness, though does suggest a potential degree of overconfidence in the ability to avoid exposure.

Despite these hazards, telecoms businesses are increasing their earnings in Africa. How are they avoiding the pitfalls?

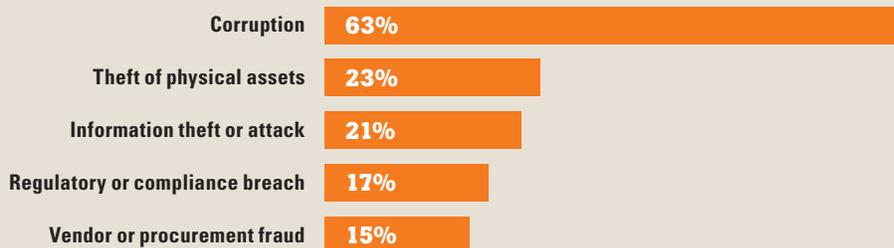
First, it is essential not to generalize. With over a billion people and more than 50 countries, conditions vary dramatically. Nigeria, for example, is historically high-risk but its government is working to manage corporate fraud. Its laws and code of corporate ethics are in line with international standards which, for listed companies, local regulators are increasingly willing to enforce.

As successful long-term investors in Africa have learned the hard way, fraud in high-risk countries can be minimized by establishing and enforcing adequate controls.

By way of example, steps implemented by leading multinationals to mitigate risk of fraud in Africa include:

- A clear demarcation of duties between senior officers, in particular the general manager and the finance manager, and a clear chart of authority within the company are essential.
- Management will need good computer software, regular internal and external audits, thorough financial management

**The risks are also large. In the survey, Africa is tied with China as the location where fraud has dissuaded most investors (11% of all respondents). For those dissuaded from operating in Africa, the top 5 causes are:**



and inventory control systems, and a procedure to verify that customers and suppliers are who they claim to be.

- A hotline for staff to report suspected fraud should be established and staff trained and encouraged to use it.
- A cross-functional leadership team must review risk management performance regularly to ensure that systems are not only in place but are being applied.



**Paul Adams**, a senior director, is the Africa specialist in Kroll's Business Intelligence and Investigations practice in London. Since joining in 2005, he has managed investigations across sub-Saharan Africa involving due diligence, political risk, market entry analysis, litigation support, competitor intelligence and anti-corruption compliance in most major industries. He was previously a journalist with news organizations including the Financial Times and Reuters in London, Lagos, Abidjan, Jakarta, Singapore and Johannesburg.

**ECONOMIST INTELLIGENCE UNIT REPORT CARD**

**TECHNOLOGY, MEDIA & TELECOMS**

The Technology, Media and Telecoms sector is facing a growing fraud threat, but has been slow to realize the danger. The incidence of all but one type of fraud covered in the survey rose in the last year. Some of the growth was alarming. The proportion hit by information theft more than doubled from 15% to 37%, the third-highest figure for the sectors surveyed. Although the IT industry might be expected to face such problems, it also saw the highest levels of IP theft (27%), market collusion (22%), and even money laundering (15%). The last of these is particularly worrying, as only 3.5% of companies think that they are even moderately vulnerable to money laundering. It may suggest that fraudsters, put off by regulatory oversight in the financial services industry, are looking further afield. Unfortunately, the growing fraud risk is not being matched by greater diligence by companies in the sector. The number spending more on IT security in the industry dropped from 59% to 42%, and the sector has the fewest companies planning to invest in the next year in seven other of the 10 anti-fraud strategies listed in the survey.

**Prevalence:** Companies affected by fraud 91%

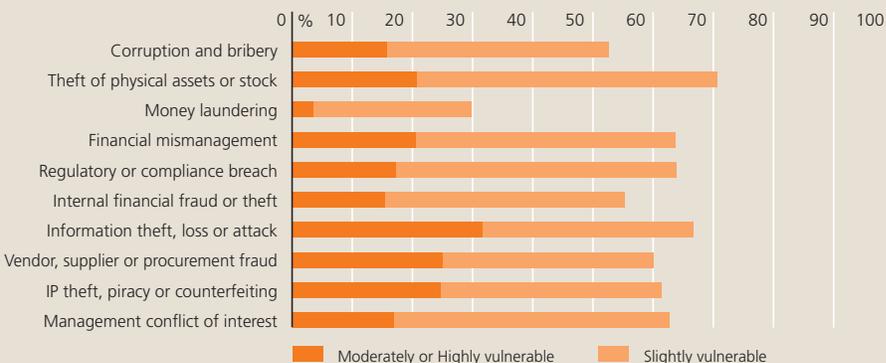
**Areas of Frequent Loss:** Percentage of firms reporting loss to this type of fraud  
 Information theft, loss or attack (37%) • Theft of physical assets or stock (27%)  
 IP theft, piracy or counterfeiting (27%) • Market collusion (22%) • Management conflict of interest (22%)  
 Vendor, supplier or procurement fraud (15%) • Money laundering (15%)

**Investment Focus:** Percentage of firms investing in prevention of this type of fraud; IT security (42%)

**Increase in Exposure:** Companies where exposure to fraud has increased 81%

**Percentage of firms investing in this type of fraud prevention in the next year:** IT security (42%)

**Biggest Drivers of Increased Exposure:** Most widespread factor leading to greater fraud exposure and percentage of firms affected; IT complexity (34%)





# Lower rates of fraud keep sector on track

The travel, leisure, and transportation sector is usually less affected by fraud than most others. This year is no exception – incidence of every fraud but one was below or near the overall survey average.

Moreover, most frauds saw a decline from last year and the one with the biggest increase – information theft, which rose from 15% to 18% – was still well below the survey average (27%). It is unsurprising therefore, that the sector had the smallest proportion of firms reporting an increase in exposure (58%).

One big fraud problem troubles this picture, however – vendor, supplier or procurement fraud (27%) affected travel, leisure and tourism more than any other industry. It has more companies that are at least moderately vulnerable to this issue (38%), but those planning to spend on the relevant due diligence (46%), while up from last year, are only slightly more than average (41%).

## ECONOMIST INTELLIGENCE UNIT REPORT CARD

## TRAVEL, LEISURE & TRANSPORTATION

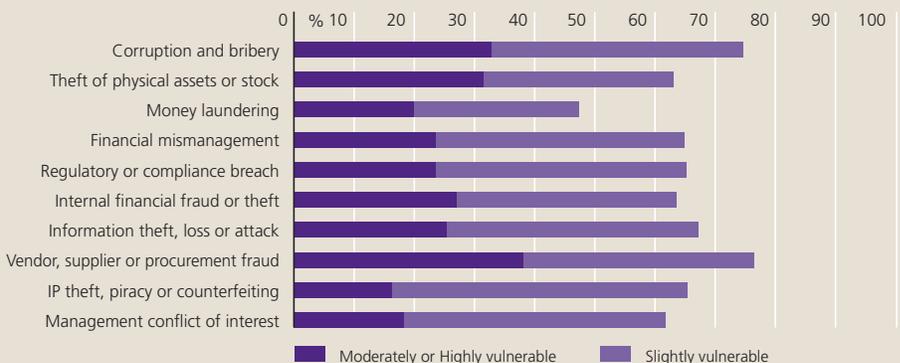
**Prevalence:** Companies affected by fraud 85%

**Areas of Frequent Loss:** Percentage of firms reporting loss to this type of fraud  
 Theft of physical assets or stock (27%) • Vendor, supplier or procurement fraud (27%)  
 Information theft, loss or attack (18%) • Management conflict of interest (15%)

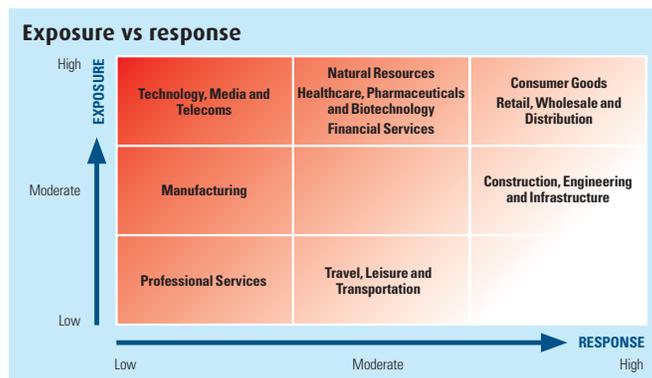
**Investment Focus:** Percentage of firms investing in prevention of this type of fraud; IT security (53%)  
 Management controls (53%) • Risk management systems (53%) • Reputation monitoring (51%)  
 Staff training (51%) • IP and trademark monitoring program (49%) • Staff screening (46%)  
 Financial controls (46%) • Due diligence (46%) • Physical asset security (40%)

**Increase in Exposure:** Companies where exposure to fraud has increased 58%

**Biggest Drivers of Increased Exposure:** Most widespread factor leading to greater fraud exposure and percentage of firms affected; High staff turnover (24%) • IT complexity (24%)



# Summary of sector fraud profiles



Sector	Exposure (degree to which sector is exposed to fraud)	Response (degree to which sector has adopted fraud countermeasures)	Comment
Technology, Media & Telecoms	High	Low	TMT companies are encountering large and growing threats from frauds of all types, as the sector faces greater exposure to information theft or loss, IP theft, market collusion and money laundering. Surprisingly, investment in fraud prevention strategies is low compared to other sectors and is concentrated on IT security.
Financial Services	High	Moderate	The exposure to fraud is broad and deep for financial services companies, which experience the greatest vulnerability to information theft and regulatory breaches. Moreover, the sector faces significant internal threats from theft of physical assets, internal financial fraud, management conflict of interest and financial mismanagement. Investment in anti-fraud measures continues to be robust though narrower than some other sectors and focuses on IT security, risk management systems and financial controls.
Natural Resources	High	Moderate	Natural Resources companies face new and significant hazards from industry trends such as increased collaboration with other firms, regulatory breaches and risks associated with new market entry. At the same time, vulnerabilities in other areas have decreased: theft of physical assets, corruption and internal financial fraud. Investment in fraud prevention strategies by companies in this sector is average and focuses on financial controls, physical asset security and staff training.
Healthcare, Pharmaceuticals and Biotechnology	High	Moderate	Healthcare, Pharmaceutical and Biotechnology companies face growing threats from information theft and IP theft as companies increasingly collaborate with other firms. Traditional areas of concern, including theft of physical assets and management conflict of interest, also continue to pose significant threats to the sector. Companies in this sector invest in a wide range of anti-fraud measures - IT security, staff training, management and financial controls, due diligence and pre-employment screening - but only at average levels.
Consumer Goods	High	High	Consumer Goods companies reported the highest incidence of fraud of the 10 sectors surveyed and suffer from the highest incidence of physical theft and fraud due to financial mismanagement. The sector also experienced an increase in information theft, adding a new dimension to its challenges. High staff turnover resulting in fraud is a persistent issue for the sector and has led to the highest adoption of anti-fraud measures: physical asset security, IT security, management controls, reputation monitoring, financial controls and due diligence.
Retail, Wholesale and Distribution	High	High	Predictably, companies in this sector struggle with high levels of physical theft and face a persistent set of issues around internal financial fraud and vendor, supplier and procurement fraud. The sector also saw a rise in the incidence of information loss or theft, which indicates a continued trend towards regarding information as a valuable and vulnerable asset. Companies in the sector reported the greatest increase in overall fraud exposure due to high staff turnover, pay constraints and weak financial controls. Investment in fraud prevention strategies mirrored these concerns: IT security, financial controls, physical asset security, IP and trademark monitoring and due diligence.
Manufacturing	Moderate	Low	Manufacturing's issues are primarily internal and staff-related as companies in this sector suffer most from theft of physical assets and vendor, supplier or procurement fraud. While the sector is characterized by a lower incidence of fraud compared with others, IP theft poses a new and growing concern. Even so, adoption of fraud prevention strategies is low in relative terms and focuses on IT security and financial controls.
Construction, Engineering and Infrastructure	Moderate	High	Construction, Engineering and Infrastructure companies suffer from high levels of management conflict of interest and corruption issues, despite the moderating effects of the prolonged economic downturn. High staff turnover contributes to other fraud exposures, including theft of physical assets, information theft or loss and vendor, supplier or procurement fraud. To combat these concerns, companies invest heavily in a broad range of fraud countermeasures such as pre-employment screening, management and financial controls, IT security and due diligence.
Professional Services	Low	Low	Professional Services companies encounter a narrow set of issues, however fraud in the sector is on the increase as companies confronted growing threats from information theft, corruption and IP theft. Despite this, investment in fraud management strategies is low compared to other sectors, with a focus on management controls and reputation monitoring.
Travel, Leisure and Transportation	Low	Moderate	This diverse sector faces fewer issues than most sectors. Areas of vulnerability include theft of physical assets, information theft and management conflict of interest. However, the most serious hazard - vendor, supplier or procurement fraud - affected the sector more than any other. Fraud prevention strategies center on IT security, management controls, risk management systems, and IP / trademark protections.

The information contained herein is based on currently available sources and analysis and should be understood to be information of a general nature only. The information is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such. Statements concerning financial, regulatory or legal matters should be understood to be general observations based solely on our experience as risk consultants and may not be relied upon as financial, regulatory or legal advice, which we are not authorized to provide. All such matters should be reviewed with appropriately qualified advisors in these areas. This document is owned by Kroll and the Economist Intelligence Unit Ltd, and its contents, or any portion thereof, may not be copied or reproduced in any form without the permission of Kroll. Clients may distribute for their own internal purposes only. Kroll is a business unit of the Altregrity family of companies.

# Key regional contacts at Kroll

## Americas

Robert Brenner  
New York  
1 212 593 1000  
rbrenner@kroll.com

## North America

David Holley  
Boston  
1 617 350 7878  
dholley@kroll.com

Jeff Cramer  
Chicago  
1 312 345 2750  
jcramer@kroll.com

Jack Weiss  
Los Angeles  
1 213 443 6090  
jweiss@kroll.com

Bill Nugent  
Philadelphia  
1 215 568 2440  
bnugent@kroll.com

Betsy Blumenthal  
San Francisco  
1 415 743 4800  
bblument@kroll.com

Jim McWeeney  
Reston  
1 703 860 0190  
jmcweeney@kroll.com

Lee Spierer  
New York  
1 212 896 2008  
lspierer@kroll.com

Dee McCown  
Houston  
1 832 631 6086  
dmccown@kroll.com

## Kroll Ontrack

Jason Straight  
New York  
1 212 833 3208  
jstraight@krollontrack.com

## Identity Theft

Brian Lapidus  
Nashville  
1 615 320 9800  
blapidus@kroll.com

## Latin America

Andrés Otero  
Miami  
1 305 789 7100  
aotero@kroll.com

Ernesto Carrasco  
Bogotá  
57 1 317 5737  
ecarrasco@kroll.com

Matías Nahón  
Buenos Aires  
54 11 4706 6000  
mnahon@kroll.com

Glen Harloff  
Grenada  
1 473 439 799  
gharloff@kroll.com

Sergio Díaz  
Mexico City  
52 55 5279 7250  
sdiaz@kroll.com

Vander Giordano  
São Paulo  
55 11 3897 0900  
vgiordano@kroll.com

## Eurasia

Tom Hartley  
London  
44 207 029 5000  
thartley@kroll.com

## Europe, Middle East & Africa (EMEA)

Tommy Helsby  
London  
44 207 029 5000  
thelsby@kroll.com

Richard Abbey  
London  
44 207 029 5000  
rabbey@kroll.com

Melvin Glapion  
London  
44 207 029 5313  
mglapion@kroll.com

Brendan Hawthorne  
London  
44 207 029 5482  
bhawthorne@kroll.com

Mike Millward  
London  
mmillward@kroll.com

Bechir Mana  
Paris  
33 1 42 67 81 46  
bmana@kroll.com

Tom Everett-Heath  
Dubai  
971 4 4496700  
teveretheath@kroll.com

Marianna Vintiadis  
Milan  
39 02 8699 8088  
mvintiadis@kroll.com

Alfonso Barandiarán  
Madrid  
34 91 310 67 20  
abarandiaran@kroll.com

## Kroll Ontrack

Tim Phillips  
London  
44 207 549 9600  
tphillips@krollontrack.co.uk

## Asia

Chris Leahy  
Singapore & Hong Kong  
852 2884 7728  
cleahy@kroll.com

Tadashi Kageyama  
Hong Kong  
852 2884 7725  
tkageyama@kroll.com

David Wildman  
Hong Kong  
dwildman@kroll.com

Violet Ho  
Beijing & Shanghai  
86 10 5964 7600  
vho@kroll.com

Richard Dailly  
Mumbai  
91 22 4244 0500  
rdailly@kroll.com

Tsuyoki Sato  
Tokyo  
81 3 3218 4558  
tsato@kroll.com

## Kroll Ontrack

Scott Warren  
Tokyo  
81 3 3218 4594  
swarren@krollontrack.com



[www.kroll.com](http://www.kroll.com)

© 2010  
An Altegrity Company