



# Global Fraud Report

---

## Economist Intelligence Unit Survey Results

The biggest threat comes from within

The battle against information theft remains a leading focus

Complacency may be the next biggest danger

Anti-corruption measures are reaping rewards

## **About the research**

The Annual Global Fraud Survey, commissioned by Kroll Advisory Solutions and carried out by the Economist Intelligence Unit, polled 839 senior executives worldwide from a broad range of industries and functions in July and August 2012. 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 Telecommunications; Healthcare and Pharmaceuticals; Travel, Leisure, and Transportation; Consumer Goods; Construction, Engineering, and Infrastructure; Natural Resources; and Manufacturing. Respondents were senior, with 53% at C-suite level. Over half (52%) of participants represent companies with annual revenues of over \$500m. Respondents this year included 28% from Europe, 26% from North America, 24% from the Asia-Pacific region, 13% from Latin America and 10% from 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

## Contents

### INTRODUCTION

Tom Hartley, President and Chief Executive Officer .....	4
--	---

### ECONOMIST INTELLIGENCE UNIT OVERVIEW

Survey results .....	5
----------------------	---

### FRAUD AT A GLANCE

Beware the enemy within .....	9
A geographical snapshot .....	10

### REGIONAL ANALYSIS: AMERICAS

United States overview .....	12
Securing your company from cyber crime .....	13
Straight talk on due diligence .....	16
Preparing for new US AML rules: Know your customers and who owns them .....	17
Canada overview .....	19
Due diligence is essential and can be more time and cost efficient than you think .....	20
Latin America overview .....	22
Risk factors in Latin American agribusiness .....	23
Brazil overview .....	25
The case for strengthening internal controls .....	26
Mexico overview .....	28
Mexico's anti-money laundering challenges .....	29
Top executives: A culture of fraud on the rise .....	31
Colombia overview .....	32
Vendor and procurement fraud in Colombia .....	33

### REGIONAL ANALYSIS: ASIA-PACIFIC

China overview .....	35
Proving staff kickback allegations: How to gather evidence efficiently .....	36
Preventing IP fraud: The better option .....	38
India overview .....	40
Procurement fraud in India: Overcoming a widespread problem .....	41
Challenges facing emerging market corporations expanding abroad .....	42
Indonesia overview .....	44
Dealing with trade secret issues .....	45

### REGIONAL ANALYSIS: EMEA

Europe overview .....	47
Bank collapses amidst mismanagement & fraud .....	48
Organized crime penetration in Italian and European businesses .....	50
Russia overview .....	52
Russia's undisclosed silent partners: Knowing who you're dealing with .....	53
The Gulf States overview .....	54
Kingdom of Saudi Arabia: Time to bridge the perception gap .....	55
Africa overview .....	57
African fraud: Understanding the risks .....	58

### SECTOR SUMMARY

Summary of sector fraud profiles .....	61
--	----

### CONTACTS

Key regional contacts at Kroll Advisory Solutions .....	62
---	----

### ECONOMIST INTELLIGENCE UNIT INDUSTRY ANALYSIS

TECHNOLOGY, MEDIA & TELECOMS .....	15
NATURAL RESOURCES .....	24
MANUFACTURING .....	27
CONSUMER GOODS .....	37
RETAIL, WHOLESALE & DISTRIBUTION .....	43
PROFESSIONAL SERVICES .....	46
FINANCIAL SERVICES .....	49
CONSTRUCTION, ENGINEERING & INFRASTRUCTURE .....	56
HEALTHCARE, PHARMACEUTICALS & BIOTECHNOLOGY .....	59
TRAVEL, LEISURE & TRANSPORTATION .....	60

# Introduction



This sixth edition of Kroll Advisory Solutions' Global Fraud Report, prepared in cooperation with the Economist Intelligence Unit, provides both heartening and sobering news for businesses around the world.

On the one hand, fraud is down globally. The proportion of companies that suffered an incident declined from 75 percent last year to 61 percent in the current survey. This surely reflects the efforts of companies to actively manage their fraud risk. However, fraud is anything but defeated, with the most common frauds, theft of physical assets and information theft (reported by 24 percent and 21 percent of companies respectively), remaining stubbornly persistent and widespread.

The data we collected this year highlight some points of particular note:

» **The biggest threat comes from within.**

Fully two-thirds of firms in our survey that were hit by fraud during the past year cited an insider as a key perpetrator, rising from 60 percent last year and 55 percent in 2010. Partly, this reflects the ease with which employees, agents or other company representatives can access confidential corporate information. But it also suggests that anti-fraud energies have been directed to putting up fences to protect from external threats which can sometimes be easier to address than facing the reality of the threat from within.

» **The battle against information theft remains a leading focus.** The menace of information theft is becoming more global. New technologies make financial or precious intellectual assets easier to transmit and store, but also easier to steal and resell. According to our survey, 30 percent of companies say they are most vulnerable to information theft and cite IT complexity as the leading cause of heightened risk exposure.

» **Complacency may be the next biggest danger.** Our survey suggests that any company can be a victim of fraud, however the data show that concerns about fraud are abating as the prevalence declines. In our experience, letting down one's guard can have dire consequences. Companies must remain vigilant as the methods and tools employed by fraudsters continue to evolve.

» **Anti-corruption measures are reaping rewards.** Companies are making gains through robust efforts to combat bribery and corruption. Half of our respondents have monitoring and reporting systems to assess risks on an ongoing basis; train their senior managers and other representatives to become familiar and compliant with the US Foreign Corrupt Practices Act and UK Bribery Act; and include a review of these laws in their due diligence, when considering an acquisition, joint venture or providing financing.

Throughout the 40-year history of Kroll, our mission has been to help clients achieve a deeper understanding of the underlying facts in a range of situations and to assist with solutions. Increasingly, fraud exhibits industry-specific and regional characteristics, which require detailed knowledge of a market, sector, business process or culture to unearth, redress and prevent. Our global team, on the ground in 17 countries, has the experience in fraud prevention and detection to deliver that mission today.

I hope this report provides some useful insights and helps you identify emerging threats and opportunities for your own business.

**Tom Hartley**  
President and Chief Executive Officer  
Kroll Advisory Solutions

# Economist Intelligence Unit Overview

## A changing fraud environment...



The sixth annual Economist Intelligence Unit Global Fraud Survey, commissioned by Kroll, polled more than 830 senior executives worldwide from a broad range of industries and functions. As in previous years, the survey tells the story of a changing fraud environment, with dangers ebbing and flowing in often unpredictable ways. This year, the data reveal five key insights.

Chart 1. Percentage of companies affected by the following frauds

	2012	2011
Theft of physical assets	24%	25%
Information theft	21%	23%
Management conflict of interest	14%	21%
Vendor, supplier or procurement fraud	12%	20%
Internal financial fraud	12%	19%
Corruption and bribery	11%	19%
Regulatory or compliance breach	11%	11%
IP theft	8%	10%
Market collusion	3%	9%
Money laundering	1%	4%

Chart 2. Proportion of all companies describing themselves as highly or moderately vulnerable to the following frauds, this year and last year

	2012	2011
Information theft	30%	50%
Regulatory or compliance breach	28%	41%
Theft of physical assets	26%	46%
Internal financial fraud	26%	38%
Vendor, supplier or procurement fraud	24%	42%
Corruption and bribery	24%	47%
Management conflict of interest	23%	44%
IP theft	21%	40%
Market collusion	15%	31%
Money laundering	13%	25%

Chart 3. Proportion of companies describing themselves as highly or moderately vulnerable to the following frauds this year, differentiated by whether they suffered a fraud in the last 12 months or not

	Suffered a fraud	Did not suffer a fraud
Information theft	39%	16%
Regulatory or compliance breach	36%	14%
Theft of physical assets	36%	11%
Internal financial fraud	35%	12%
Vendor, supplier or procurement fraud	34%	8%
Corruption and bribery	33%	10%
Management conflict of interest	31%	11%
IP theft	27%	11%
Market collusion	22%	5%
Money laundering	19%	4%

## 1. Prevalence and cost of fraud are down from last year, but more than six in every ten companies were still hit at least once.

The most striking result of this year's survey is that there has been a notable decline in the level of fraud overall. The proportion of companies reporting that they were affected by at least one incidence of fraud in the past year has dropped for the second year in a row, from 75% to 61%. The average cost of fraud to businesses has declined even more, from 2.1% of revenues to 0.9%, and the number of companies saying that their exposure to fraud has increased in the past year is also down, from 80% to 63%. The picture is similar across regions and industries.

Of course, change never happens evenly. A look at the specific frauds covered by the survey shows that the theft of physical assets and information remains nearly as widespread as ever. The big drops came instead in procurement fraud and corruption, the latter probably due to increased vigilance (see chart 1).

This improvement, though, should not obscure the fact that, for companies, suffering from fraud remains very much the rule rather than the exception. More than six in 10 companies were affected last year and a similar number saw their risk of being hit by fraud increase. More importantly, the overall picture contains significant trouble spots. Manufacturing, for example, experienced a substantial jump in the number of companies suffering from fraud, going from 74% to 87%.

## 2. Concern about fraud is dropping faster than fraud itself. Companies need to avoid becoming complacent.

One concern arising from this year's survey is that companies' sense of vulnerability to fraud is decreasing even faster than its incidence.

In particular, the number of respondents saying that they were moderately or highly vulnerable to information theft has fallen from 50% to 30%, even though only 2% fewer companies reported being hit by this fraud. Moreover, the percentage of companies concerned about the theft of physical assets is now only a little higher than the proportion that has actually suffered from such a crime in the past year.

Is this change in perception simply an understandable, if perhaps excessive, reaction to lower fraud levels? The survey data

suggests something more: a sense of the risk of fraud is often based not on a dispassionate assessment of the environment, but on recent direct experience. Companies that suffered any sort of fraud in 2012 are more likely to see themselves as vulnerable.

This tendency for risk assessment to be reactive can lead to dangerous complacency when luck, more than diligence, may be the reason for avoiding fraud. In an environment where a majority of companies have suffered from a fraud in the last year, becoming over-confident presents a substantial risk. A lack of attention can be costly: companies that lose the most to fraud are those that are less likely to have fraud controls in place.

### 3. The biggest danger still comes from inside the business.

Increasingly, fraud is being perpetrated by company insiders. Previous surveys have consistently indicated that insiders are responsible for most frauds. More than two-thirds (67%) of firms that have suffered at least one incidence of fraud in the past year cited an insider as the key perpetrator or one of the leading culprits, up from 60% last year and 55% the in 2010.

The findings also shed light on how fraudsters interact by asking companies about all the perpetrators involved, not just the most significant one. From the data it was possible to isolate a large group of companies—more than 200—that reported being affected by just one type of fraud. Members of this group are the most likely to have suffered a single fraud or series of frauds by the same perpetrator or perpetrators.

Looking at who committed these frauds, the most obvious finding is that fraudsters tend either to act alone or to co-operate with peers rather than with members of other groups. Respondents cited just one type of leading perpetrator in 84% of cases. These were, as expected, usually an insider. Those acting alone in this way tended largely to be insiders—junior employees, senior managers, or agents of the company.

In the smaller number of cases where different types of perpetrators co-operated, the tendency was again to bring in as few people as possible: 83% of such cases involved only two types of perpetrators, presumably because secrecy is easier to maintain with fewer participants in a scam.

Chart 4. Percentage of companies that have fraud controls in place

	Companies that lost more than 4% of revenues to fraud	All other companies
Financial (financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)	61%	82%
Assets (physical security systems, stock inventories, tagging, asset register)	57%	75%
Information (IT security, technical countermeasures)	55%	80%
Management (management controls, incentives, external supervision such as audit committee)	45%	73%
Staff (training, whistleblower hotline)	43%	65%
Partners, clients and vendors (due diligence)	43%	62%
Staff (background screening)	37%	65%
Reputation (media monitoring, compliance controls, legal review)	37%	62%
Risk (risk officer and risk management system)	31%	68%
Incident response plan for data breach	29%	58%
IP (intellectual property risk assessment and trademark monitoring programme)	25%	54%

Chart 5. Percentage of companies affected by multi-perpetrator frauds reporting the following types of perpetrators (2012)

Suppliers	43%
Vendors	37%
Junior employees of our own company	29%
Customers	26%
Agents and/or intermediaries	23%
Government officials	20%
Regulators	17%
Senior management employees of our own company	11%
Partners	6%
Other	3%

When a fraud involves more than one type of perpetrator, though, outsiders are much more involved and, except for junior employees, insiders are much less so.

There is insufficient data to examine the types of combinations in great detail but it is worth noting that 37% of these multi-perpetrator frauds involve a combination of insiders and outsiders, and that only rarely (11% of the time) do insiders of different types work together. Of the outsiders, vendors and suppliers frequently work together, doing so in 29% of all multi-perpetrator cases. The broader message is

that, although insiders can often find ways to defraud the company by themselves, external fraudsters tend to look for accomplices.

### 4. Information theft remains a significant, multi-faceted threat.

As in previous years, information theft is one of the most widespread frauds facing companies. Its modest decline – 21% of companies are affected this year compared with 23% in the last survey – shows that it is more resilient than some other frauds. Moreover, it remains the fraud to which respondents feel most vulnerable – 30% say

they are moderately or highly so. It is also a problem which has the potential to grow: IT complexity is the leading cause of increased exposure to fraud risk, according to 30% of respondents.

The popular perception of information theft typically involves hackers stealing reams of customer data. This is certainly an issue but the threat is not one-dimensional. To begin with, a range of information is being sought by different fraudsters, with customer data an important, but not the most frequent, target: one-third of all those suffering an information attack lost such data in the last year. On the other hand, 46% have had either company financial data or strategic data stolen. And the focus of attacks varies widely by industry. In the professional services sector, for example, 49% of attacks involved a search for financial or strategic data, while only 33% sought customer data. In financial services, on the other hand, the equivalent figures were more equal – 46% and 50% respectively. The broader message is that a wide range of information is valuable and therefore under threat in the era of ‘Big Data’.

Employees – either as culprits or as a point of weakness – are far more to blame for the loss of information than hackers. Where there has been a loss, 35% of the time the issue is employee malfeasance, more than twice the rate at which external hackers are to blame (17%). Moreover, in 51% of cases, the theft of an employee’s technology (such as a computer or mobile phone) or an employee mistake was involved. As ever, though, these are average pictures and individual countries can have distinct risk environments: Indonesia saw the most companies affected by information theft (35%) while outside hacker attackers were the most common in the United States, affecting 10% of all companies.

## 5. Taking anti-corruption compliance more seriously is paying dividends for companies.

The impact of the US Foreign Corrupt Practices Act (FCPA) and UK Bribery Act is growing, with companies taking steps to improve their compliance. Compared with last year, far more have done a risk assessment relating to these pieces of legislation, trained senior managers appropriately and integrated corruption issues into their due diligence activities. As a result, anti-corruption policies are becoming more widely embedded in many businesses.



Chart 6. Percentage of companies agreeing with the following

	2012	2011
<b>We have made a thorough assessment of risks to our organisation arising from the UK Bribery Act and/or US FCPA and their enforcement, and set in place a monitoring and reporting system to assess risks on an ongoing basis.</b>	52%	26%
<b>We have trained our senior managers, vendors and foreign employees to become familiar and compliant with the UK Bribery Act and/or US FCPA.</b>	55%	29%
<b>When entering into a joint venture, making an acquisition or providing financing, our due diligence includes a review of UK Bribery Act and/or US FCPA risks.</b>	50%	26%
<b>Our internal compliance regime is becoming more global because of the extraterritorial reach of the UK Bribery Act and/or US FCPA.</b>	56%	26%

This still leaves room for improvement. More than 20% of respondents say that although they are subject to the UK Bribery Act or US FCPA, they have not made a thorough risk assessment, trained the right people or amended their due diligence process. The survey data suggest that in failing to take these steps, companies may be missing out. The marked rise in compliance activity has coincided with a fall in the prevalence of corruption from 19% to 11% during the past year. Companies with active compliance seem to have benefitted more. Of those respondents who say that they have trained employees and others to comply with

anti-corruption legislation, conducted a risk assessment and integrated corruption considerations into their due diligence processes, only 7% reported suffering from an incidence of corruption compared with 13% of all other companies.

Just as importantly, such compliance regimes may also be opening up investment opportunities for companies. Of the companies which had taken all of the above steps, only 20% were dissuaded from investing abroad because of fraud, but for those who have not taken these steps the figure was 31%. Better anti-corruption efforts seem to bring substantial benefits.

# Beware the enemy within

By Tommy Helsby

**This year's Global Fraud Survey reinforces last year's result: senior executives do not perceive an increasing risk of fraud. Newspaper headlines seem to tell a different story: LIBOR-fixing in London; bribery and money laundering in Mexico; accounting fraud in Tokyo; bank fraud in, well, almost everywhere. Why the discrepancy?**

The frauds that excite the newspapers are essentially frauds by the company rather than on the company. When corporate executives think about fraud, the natural response is to consider ways in which their businesses could be victims, and not how their companies could be committing fraud. But a moment's reflection shows that most firms that have, in newspaper terms, "committed a fraud" are also victims of the fraud's consequences.

At best, the fraud creates a short term gain – a contract won through a bribe, a commercial advantage through collusion with a competitor, or concealment of a financial problem through accounting fraud. But the long term consequences are invariably bad for the business – worse if the fraud is discovered and the company has to pay the penalties, but bad even if they "get away with it." As I commented in last year's Report, business based on bribery, uncompetitive practices, or unethical practice is unsustainable in the long term: it lacks integrity in the commercial as well as the moral sense.

A prevailing concern among our clients is that there may be someone within their organization who is breaking the law as part of their job; perhaps believing that they are simply doing the right thing; possibly unaware that their actions are illegal. The common reaction when such activity is discovered is that "everybody does it," or "it's market practice," or "that's the only way to survive in business here," or "I was doing it for the company." In many cases, the offending employee does not benefit, other

than perhaps by getting a better bonus, but the company has benefited, in the short term, and will be held responsible, by regulators, law enforcement and the media.

There is no water-tight defense against this problem. Perhaps it's possible to avoid in a small business, where the boss knows every employee and can see every action, but in a modern multinational corporation there will always be some level of vulnerability to what we call "corporate hero fraud." There are two mitigating strategies: effective compliance and independent internal investigation.

To be effective, compliance needs to operate on a series of levels and cannot be the responsibility only of the compliance department: compliance is a core management duty that crosses all corporate functions. It needs involvement from human resources, finance, legal, internal audit and, ultimately, senior management. Employees need training in what is and is not acceptable practice within the company; no one can be allowed to get away with saying, "I didn't know it was wrong." Practices need to be reviewed against legal and regulatory developments. Activity needs to be monitored and, since it's generally impractical to monitor everything all of the time, it will involve testing and developing systems to pick up improper behavior: you need a defense against an accusation of "turning a blind eye" to illegality. There need to be robust procedures in place to respond to potential issues, but in a nuanced and proportionate way. Heavy-handed and hair-trigger responses can be counter-productive: people will be less

inclined to report possible issues if the automatic result is an aggressive and disruptive internal investigation.

Establishing effective internal investigation procedures is vital. With most business processes now being electronic, there will be much preliminary work that can be done with little disruption, such as email reviews and data mining (although beware of any applicable privacy laws). Some basic checking can establish whether an issue is a problem heading towards something bigger, and prompt action can often head it off if it is serious. As important as the practical skills are, it is also vital to think through the context, purpose, and consequences of an internal investigation. Who is affected by the issue – just the company or third parties such as customers or suppliers? Will the results need to be shared with a regulator, either immediately or at some later date? Could the results lead to litigation for financial recovery, or to a criminal complaint? Are the scope and terms of reference appropriate?

For example, I have had calls from clients who want to identify the sender of a poison pen letter – a reasonable task, but one man's poison pen letter writer is another's whistleblower. Such a project needs to be handled with care, and it may be important to first address the issues raised in the letter in order to establish whether there is a genuine issue, however maliciously raised.

Thinking through these issues will help in deciding whether, and at what point, to bring in external help. If you need to demonstrate to third parties, whether regulators or customers, that a thorough investigation has been conducted, doing everything in-house may lack credibility. In other cases, leaning on the experience of a team that has dealt with similar cases before can be critical (and reassuring). An intimate understanding of the company may be equally important, and so a combined team may be the best approach.

Thinking that fraud can't happen to you means that it probably will, or already has. The best attitude is to be prepared: spot it early, respond effectively, and learn from the experience.



**Tommy Helsby** is Chairman, Eurasia of Kroll Advisory Solutions 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.

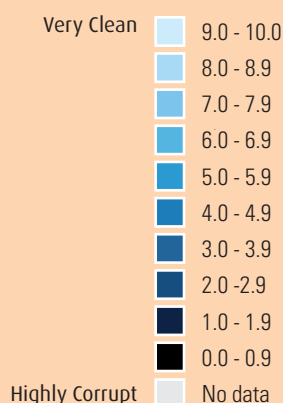
# A geographical snapshot

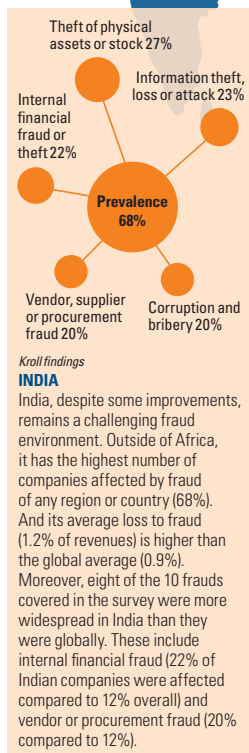
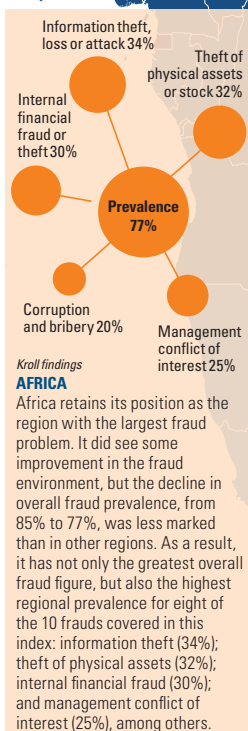
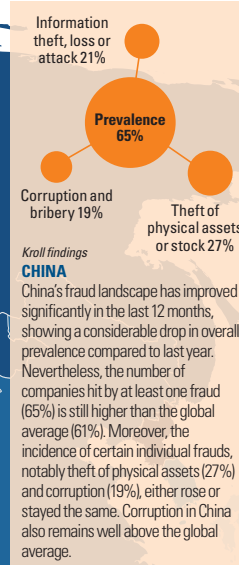
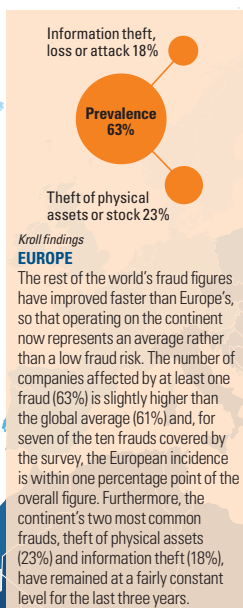
We compared the results of the Global Fraud Survey findings with Transparency International's Corruption Perceptions Index (CPI). The CPI measures the perceived levels of public sector corruption as seen by business people and country analysts; ranging between 10 (very clean) and 0 (highly corrupt).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





# UNITED STATES OVERVIEW



American companies shared in comparatively little of the global improvement in fraud levels over the last year. The number of US businesses hit by at least one fraud was down (to 60% from 65%) and the average loss also dropped (to 1.1% of revenue from 1.9%), but these declines were much less than the global average.

	2011-2012	2011-2010
<b>Prevalence:</b> Companies affected by fraud	60%	65%
<b>Areas of Frequent Loss:</b> Percentage of firms reporting loss to this type of fraud	Information theft, loss, or attack (26%) Theft of physical assets or stock (24%) Management conflict of interest (16%)	Information theft, loss, or attack (27%) Theft of physical assets or stock (24%) Management conflict of interest (16%)
<b>Areas of Vulnerability:</b> Percentage of firms considering themselves moderately or highly vulnerable	Information theft, loss or attack (33%) Regulatory or compliance breach (29%) Vendor, supplier or procurement fraud (27%)	Information theft, loss or attack (52%) IP theft (39%) Theft of physical assets or stock (36%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	66%	79%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	IT complexity (35%)	IT complexity (35%)
<b>Loss:</b> Average percentage of revenue lost to fraud	1.1%	1.9%

Moreover, the prevalence of the four most common frauds – information theft (26%), theft of physical assets (24%), management conflict of interest (16%), and procurement fraud (13%) – are largely unchanged from last year.

Information theft remains the biggest threat and the complexity of information technology the biggest driver of increased fraud in the country. American companies are among the most likely in the world to report an attack by an outside hacker – with 10% of all US respondents hit in this way within the last 12 months. However, despite a threat which saw little change in prevalence in the last year, the number of companies thinking that they are moderately or highly vulnerable to information theft dropped from 52% to just 33%.

In fact, for all the four leading frauds listed above, despite static prevalence figures, the sense of vulnerability dropped markedly.

## Proportion of US companies describing themselves as highly or moderately vulnerable to the following frauds.

	2012	2011
Information theft	33%	52%
Theft of physical assets	20%	36%
Management conflict of interest	25%	34%
Vendor, supplier or procurement fraud	27%	31%

American companies may need to challenge any assumptions about living in a low-fraud environment. For half of the frauds covered in the survey, the prevalence in the United States this year was higher than the global average. Moreover, the average amount lost to fraud, 1.1% of revenues, is now higher than the global average of 0.9%. On the other hand, for all but one of the anti-fraud strategies covered in the survey, the percentage of American companies which have them in place is lower than the global average and, for every strategy, the proportion of companies planning to invest further in the coming year is also lower. If businesses in the United States want to address their ongoing fraud issues, they will need to get more active.



Expert Q&amp;A with Mike DuBose and Tim Ryan

Undetected malware, a misplaced mobile device, a hacker taking sensitive data hostage – cyber security threats today are increasing in variety, frequency, and sophistication. This endless range of vulnerabilities makes it nearly impossible to predict the location of your organization's next security breach. The Global Fraud Report spoke with Mike DuBose and Tim Ryan, cyber investigations and security experts with Kroll Advisory Solutions, about this complex threat to critical business assets such as intellectual property, financial and customer data, and trade secrets.

**Q. What are the most serious cyber threats that companies face?**

**Mike:** The list keeps growing, unfortunately, but some of the top ones come from organized crime groups in Eastern Europe and Asia. Many of these groups control botnets that exploit the machines of hundreds of thousands of innocent computer users, increasing the reach and scale of their criminal enterprises to unprecedented dimensions. They employ whatever hacking methodology works, often tailored to specific targets of opportunity. Phishing schemes, mobile device exploits, advanced persistent threats, social engineering, SQL injections – all are attack modalities that companies need to prepare for and address expeditiously.

**Tim:** The internal cyber threat is also severe. It may come from a disgruntled employee who steals trade secrets before leaving for another job or a vengeful systems administrator who sabotages the network after hearing about his termination. It is made worse when a company's leadership –

including the CEO, CFO, and the Board – fails to appreciate the magnitude of the cyber threat and gives it inadequate prioritization and resources.

**Q. Which cyber crime trends should especially worry businesses?**

**Tim:** Cyber-based data destruction events are increasingly common. In these events, attackers destroy or ransom a corporation's data. In other words, rather than stealing a corporation's intellectual property, these attackers forensically destroy data, making its recovery difficult. This causes enormous injury to companies, including significant disruption to the continuity of business operations that can lead to lost production, lost revenue, remediation costs, and reputational damage.

**Mike:** We are also seeing more economic espionage, much of it again originating in Eastern Europe and Asia. Some is state-sponsored. These cyber attacks target a company's trade secrets, confidential

communications and financial documents – virtually any digital asset that can be used for market advantage. Some of the newest and fastest growing targets for these criminal groups are mobile computing devices [see box overleaf].

**Q. What are these hacking groups after? Is there specific information about which companies should be especially concerned?**

**Mike:** As much as I hate to give this response, it depends. There are variations among industries, but generally hackers are after almost any type of data or digital business asset that can be used to obtain financial gain or competitive advantage in the marketplace. The exceptions are the so-called hacktivist groups which disrupt networks or publish sensitive internal data in the name of a cause.

**Tim:** Attackers engage in hacking for a variety of reasons. The same motives that exist in the real world also exist in cyberspace – only the venue has changed.

## The Employee Dimension

### Q. What challenges do social networking and mobile devices pose and how can a business protect itself?

**Mike:** Social networking enables attackers to find and exploit personal information posted to social networking sites, as well as to exploit the trust relationships that develop between people on such sites. This can pose a variety of big problems for businesses. For example, more and more companies are experiencing targeted phishing attacks (or “spear phishing”). Their employees receive phishing emails with innocent looking attachments or embedded links that appear to be business-related; clicking on them downloads malware to the network. Emails that appear to be from a contact on a social network may be viewed as more trustworthy than an email from an unidentified source. Moreover, social network sites that reveal an employee’s professional information can make them more susceptible to spear phishing attacks. One example is if a system administrator, who normally has access privileges to a company’s entire network, reveals his employer and his position title on LinkedIn; that individual’s email account and computer become a more attractive target for a hacker seeking to gain access to the company’s most sensitive data.

Mobile devices – smart phones, iPads, and the like – are the new frontier for hacker groups. According to one study, in the first quarter of 2012 alone, over 3,000 malicious Android application packages and 37 new Android malware variants were created, nearly four times the number seen in the first quarter of last year. Meanwhile, these devices have caused an expansion in the borders of the corporate IT infrastructure. Mobile applications and Bring Your Own Device policies have blurred the line between corporate and personal computing. In a sense, professional IT security has been forced into an uneasy partnership with personal user habits, as personal use and corporate use increasingly occur on the same mobile device. Corporate information can reside on so many different devices that understanding the full scope of the network, much less the security risks, is simply more difficult today than it ever has been.

**Tim:** There’s no one-size-fits-all solution for the risks these trends present but, in general, corporations should stick to security fundamentals: build IT systems that are resilient to attack; understand how a security tool or managed service fits into the overall security strategy; educate employees on a regular basis on best practices for safe computing. It is now important as well to verify your cloud providers’ security measures before trusting them with sensitive data. Remarkably, a recent study by the Ponemon Institute found that 74% of surveyed IT compliance officers had selected, or would select, cloud providers without first vetting their security practices. Unfortunately, if past is prologue, it will take several very large, very public breaches of cloud provider systems to meaningfully change corporate behavior in this regard.

Any number of motives may prompt an attack: hackers may be after business intelligence and intellectual property for competitive advantage or financial gain; they may exploit vulnerable systems to embarrass corporations for purely ideological reasons; sometimes, they may seek to destroy infrastructure for personal reasons, including revenge. Of course, one should secure any form of financial information that an attacker could leverage to steal money, but the landscape of targeted data is evolving and growing. It is not enough to be concerned about how sensitive data is stored and accessed. Corporations must be equally vigilant in strengthening IT infrastructure in order to preserve business continuity.

### Q. Are hackers targeting some types of organizations more than others?

**Mike:** Some industries or organizations may be more at risk than others depending on the type and amount of data they store, but almost all companies store information that outsiders could use for financial gain or market advantage. So, all are at risk. The size of the company doesn’t seem to matter anymore. Hackers are targeting mid-sized to small firms with greater frequency, perhaps because their network security is lagging behind the improvements implemented by some of their larger competitors. Hacking groups will gravitate toward victim networks that are more easily breached. Thus, a small health care provider may face risk equal to,

or greater than, that of the largest hospital, and a regional bank may experience attacks equal in severity to those experienced by a large international banking institution.

### Q. How can companies improve their cyber security?

**Mike:** A good place to start is to commission a comprehensive cyber risk assessment by a qualified firm, including penetration testing and a thorough review of security protocols. Of the hundreds of such risk assessments Kroll has conducted, there has never been one in which security measures could not be improved. In terms of preparing for a breach investigation, companies might want to conduct a comprehensive network mapping exercise that shows all system connectivity and the location of the company’s most valuable digital assets. It’s surprising the number of cases we’re called in to where there isn’t an accurate network map or even institutional knowledge of where the businesses’ assets are located on the network. This information is one of the first things we ask for when we investigate a data breach.

More generally, cyber security needs to be one of the highest priorities for any organization – with senior executive responsibility, Board review, and proper resource allocation. Moreover, businesses must understand that compliance with industry regulations is insufficient, by itself, to ensure adequate data and network security. Until an organization’s cyber security is given the same importance as net profits and EBITDA margins, even the most carefully-crafted cyber security policy will fail to produce the type of widespread change in corporate culture that is necessary to meet today’s cyber threat.

**Tim:** Companies can start by having a comprehensive understanding of their infrastructure, data, and processes. From there, they can implement best practices and a thoughtful security policy to harden their environment to help withstand attacks, as well as to alert all relevant parties and decision-makers when a breach is detected or suspected. All of this depends on creating a professional security component within the organization. Keeping systems and data secure is a professional responsibility requiring all the attendant training, certification, quality assurance, and investment that accompanies other essential business functions.

Combined with well-trained people, putting the correct technology in place is also absolutely essential. It is the difference between trying to solve a crime by merely viewing shoeprints at the crime scene and seeing the actual event with real-time video footage. This greatly enhances the speed at which intrusions can be detected and mitigated. Also, implementing the appropriate security technology increases the cyber infrastructure's resilience as a whole. In the end, preventing the breach is the priority.

### Q. What are some of the common mistakes that companies make in this field?

**Mike:** When responding to a security breach, some companies tend to want narrower investigations because they believe that broader ones expose more vulnerabilities, which, in turn, could increase corporate liability. However, very often quite the opposite is true. For example, after a hacking incident left a client's network exposed for three months, the company was prepared to notify the over 250,000 customers whose credit card numbers and PINs had been processed during that time. Fortunately, before sending out the notification letters, they called Kroll about credit monitoring services. We recommended that another step needed to be taken before notification: validation of the initial investigation.

When our forensics experts reverse-engineered the code used to compromise the data, we discovered that only one type of credit card had been targeted and that a bug had caused the malicious code to stop working after only 21 days.

Thus, we narrowed the scope of exposure from three months to three weeks, and reduced the number of impacted individuals—and notifications required—from over 250,000 to less than 30,000. The client's cost to meet mandated notification requirements was reduced by 90% at a savings of more than \$1.3 million.

**Tim:** Many companies incorrectly assume that regulatory compliance equates to adequate network security. Others invest in cyber security only after a breach has occurred. The biggest mistake, however, is the assumption that the same system administrators who get their systems to work daily are also capable of investigating data breaches. While many are adept at keeping IT systems running, most would tell you that investigating a breach or attack is not their forte. They just don't have the experience in

what is a highly complex task. Rarely at the outset of an investigation is the full scope and cause of the incident known. Attacks that initially appear to be external only later may be proved to be caused by an insider. Breaches that at first seem confined to one network location frequently lead to the discovery of malware infections at other locations on the network. The scope of the investigation constantly needs to be reassessed and examined to account for new evidence. At the end of the day, cyber attackers are human, and a thorough investigation needs to enlist the full spectrum of investigative capabilities—from sophisticated computer forensics to boots-on-the-ground investigative techniques.

Hoping that in-house IT will be sufficient here has proven disastrous for many corporations. Studies have shown that over three quarters of corporate hacking victims have been informed of a breach in their systems from a third party, such as law enforcement or a major Internet service provider. Upon investigation, these companies usually find that the infection has resided on their system

for months, if not years, sometimes stealing or destroying huge quantities of sensitive data. Many of these companies had excellent IT teams who ensured continuity and efficiency in business operations, but they weren't trained to deal with the types of cyber threats companies now face.

**Michael DuBose** is a Managing Director and Head of Kroll's Cyber Investigations Practice. Michael previously served as Chief of the Computer Crime and Intellectual Property Section at the United States Department of Justice, where he managed some of the largest investigations and prosecutions ever brought in the U.S. involving computer network intrusions, international phishing schemes, botnets, hacktivist groups, copyright piracy, theft of trade secrets, and large-scale data breaches.

**Timothy P. Ryan** is a Managing Director with Kroll's Cyber Investigations Practice based in New York. An expert in responding to all forms of computer crime, attacks, and abuse, Tim previously was a Supervisory Special Agent with the Federal Bureau of Investigation, where he supervised the largest Cyber Squad in the United States. Tim has led complex cyber investigations involving corporate espionage, advanced computer intrusions, denial of service, insider attacks, malware outbreaks, Internet fraud and theft of trade secrets.

## ECONOMIST INTELLIGENCE UNIT REPORT CARD

## TECHNOLOGY, MEDIA & TELECOMS

The fraud challenges facing the technology, media and telecommunications sector are slightly greater than for other sectors. The number of businesses affected by at least one incidence of fraud in the past year (64%) and the average loss (1%) are slightly higher than the figures for the entire survey (61% and 0.9% respectively). The biggest problem, information theft, affected 26% of businesses last year, again higher than the survey average (21%), but the sector is likely to suffer more attacks than some others given that it is IT-based. If there is a specific concern about technology, media and telecommunications companies, it is whether they are ready to address future fraud threats. On one hand, for seven of the types of frauds covered in the survey, the proportion of firms that rate themselves highly or moderately vulnerable is within 2% of the survey average, and in two further types it is higher. On the other hand, these companies are noticeably less likely than average to have in place each of the eleven anti-fraud strategies covered in the survey and in nine of these cases fewer firms than average are planning to invest in such strategies in the next year.

**Loss:** Average percentage of revenue lost to fraud: 1%

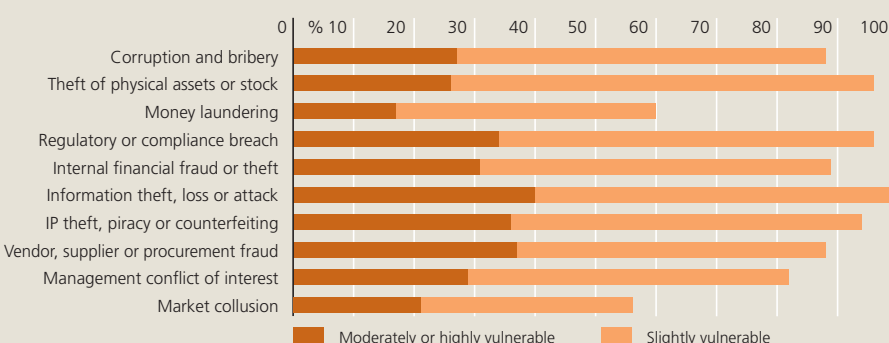
**Prevalence:** Companies affected by fraud: 64%

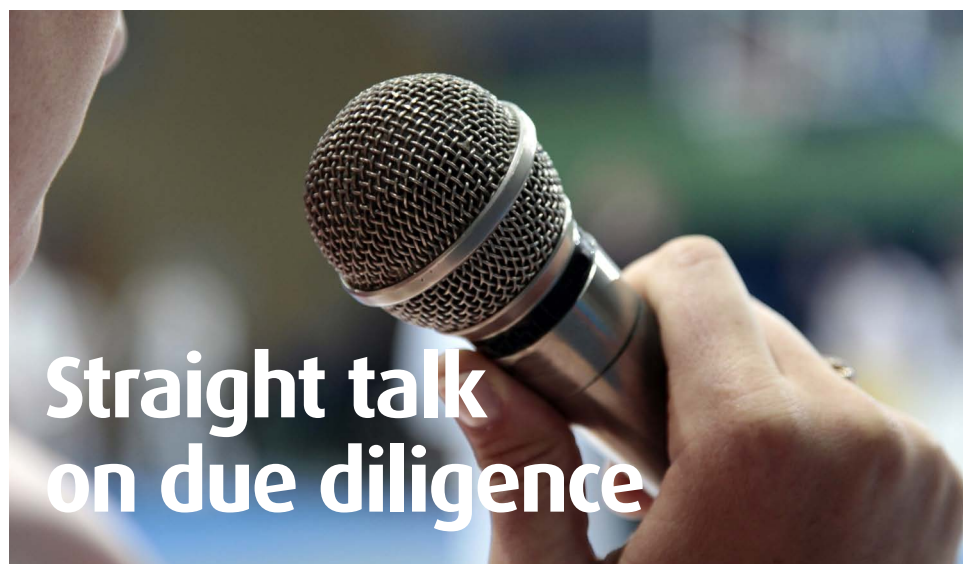
**Areas of Frequent Loss:** Percentage of firms reporting loss to this type of fraud

Information theft, loss or attack (26%) • Theft of physical assets or stock (19%)

**Increase in Exposure:** Companies where exposure to fraud has increased: 71%

**Biggest Drivers of Increased Exposure:** Most widespread factor leading to greater fraud exposure and percentage of firms affected: Entry into new, riskier markets (35%)





By Peter Turecek

A wide variety of due diligence screening and investigative offerings exist in the marketplace, all varying in scope, purpose and price. Determining the best option for a particular need requires balancing a number of factors, including the reasons for the check, the risks associated with the contemplated transaction, costs, and the timeframe for which to complete the due diligence. Measuring and weighing the factors will ultimately determine the scope of the screen or investigation. However, striking that balance between those factors is not always as easy as it may seem, and, with haste, could lead to more questions than answers.

The analysis begins with an understanding of the issues involved, and the levels of risk accompanying them. Is this a “make-or-break-the-company” transaction in which a key acquisition or partnership is contemplated? Are significant reputational risks to the company involved? Are the investigations part of an effort to implement an effective Foreign Corrupt Practices Act/UK Bribery Act program, or in connection with a Know Your Customer/Anti-Money Laundering program in which hundreds or thousands of vendors or customers need to be examined on a global basis? Or do the concerns lie somewhere in between?

Generally, due diligence screening is the process of checking names against limited available public records. At the most basic, least-risky end of the spectrum, compliance screens on straightforward subjects in stable jurisdictions may only require a check against global governmental sanctions databases and watch lists. Additional levels

of risk may escalate the scope of the screen to include additional searches such as adverse media reviews or limited searches of online public records. For programmatic compliance-driven requirements, or preliminary screening of numerous investment opportunities, these options may be the most appropriate and cost-effective due diligence measures.

Frequently, basic compliance screens need more thorough due diligence efforts. Given limited public record availability in many jurisdictions around the world, or heightened risk factors in certain regions, satisfying certain compliance requirements may necessitate additional reviews. For example, the absence of public records in most Middle Eastern countries may require reputational source inquiries. Similarly, the lack of transparency of corporate structures and beneficial ownerships in jurisdictions such as the British Virgin Islands, Lichtenstein, or Cyprus may warrant enhanced due diligence searches. Additionally, the high public profile of some subjects may drive the need for a more comprehensive understanding to address additional risks.

Due diligence efforts involving transactions of significant size, or which may have significant reputational risk, may necessitate using an investigative methodology as opposed to a screening approach. The investigative due diligence methodology follows an iterative research process, collecting information from a broad range of databases and available public records, as well as comprehensive source inquiries as needed. This data is married with critical analysis and corroboration to provide a deeper level of completeness and understanding about a potential counterparty.

While it probably need not be said, as the scope of an effort increases, so too does the cost of the investigation. However, selecting the proper level of due diligence should also acknowledge that there may be times where increasing the scope, and therefore, the price, of the examination is required. What may begin as a compliance screen, for example, may result in a full-blown investigative due diligence investigation if the results of the screen raise additional concerns for the client.

Kroll recently completed an investigation for a private equity firm considering the acquisition of a company in which the initial screen identified a state criminal record belonging to the main subject of the review. The client elected to escalate the level of due diligence inquiry in order to develop specifics about the charge and disposition of the case. Kroll’s investigation identified that the defendant was charged with stealing from a store and using violence against an employee in the process. The defendant pled guilty to petty theft. Further investigation into the defendant identified two additional criminal cases in different counties in the same state. Kroll analysts reviewed the additional case files and determined that the defendant had actually provided an alias to law enforcement – the name and date of birth of the subject of Kroll’s investigation. In fact, the real criminal defendant was a relative of the subject – a relative who had a lengthy criminal record. But for the additional analysis and investigation, the private equity firm may have mistakenly made decisions about its investment based on incomplete or false information.

Determining the appropriate level of due diligence requires examining the risks posed by the transaction and scoping the screening assignment or investigation appropriately. Ideally, the selection should balance risks with the specific details of the transaction, including the nature of the industry, geographical jurisdictions, and profiles of the subjects involved. A good due diligence provider will honestly assess the needs and make the best recommendation as to the appropriate level of effort.



**Peter Turecek** is a Senior Managing Director in the New York office. He is an authority in due diligence, multinational investigations, and hedge fund related business intelligence services. Peter also conducts a variety of other investigations related to asset searches, corporate contests, employee integrity, securities fraud, business intelligence, and crisis management.

# Preparing for new US AML rules: Know your customers and who owns them

By Nikki Kowalski

With the release of the Advance Notice of Proposed Rulemaking (ANPR) in February, United States anti-money laundering (AML) regulators signaled that in the future, American financial firms will need to know more about the individuals who own and control the entity-type clients with which they do business. These include corporations, partnerships, trusts, and similar structures. While the government and the financial services industry debate the exact contours of any enhanced requirements regarding the identification of so-called “beneficial owners” of these clients, what should AML departments do now to prepare for this change?

The ANPR is just the latest expression of regulators' evolving views on the subject of beneficial ownership. An important goal of the Bank Secrecy Act (BSA) is to identify and deter suspicious activity in the financial system. FinCEN, the bureau within the Treasury Department charged with administering BSA compliance, has long held that in order to be able to distinguish between normal behavior for an entity-type client and unusual or potentially suspicious activity, a financial firm needs to know who owns or controls the entity.

Nevertheless, current BSA regulations explicitly require identification of the beneficial owner of an account in only a few circumstances: for private banking accounts and for certain accounts held by non-US financial institutions. In the past, FinCEN has explained the absence of further requirements as necessary to allow financial institutions to fashion risk-based, customer diligence practices appropriate to their own customer mix.

This approach to rulemaking earned the United States a rating of only "partially compliant" with international standards on customer diligence in a 2006 mutual evaluation conducted by the Financial Action Task Force (FATF). Since then, FATF recommendations for international best practices have been revised to call for even more transparency in identifying who owns and controls entity-type clients.

The ANPR represents a significant effort to bring American rules more in line with international standards. It also seems to be belated recognition by regulators that, in the absence of explicit requirements, some financial institutions may not have been collecting the information about ownership and control of entity-type clients that they need, in order to conduct an informed risk analysis of the customer.

The ANPR has several components but, in general, it proposes the identification of individuals who own more than 25% of an entity. If no one meets this threshold, then those who own as much as any other individual should be identified. In addition, the individual primarily responsible for directing the affairs of the entity should be

identified. During the public comment period on the proposal in the spring and summer of 2012, the financial services industry offered constructive suggestions about how some of the details of the proposal might be improved, and provided informed feedback on the likely cost of such an undertaking. Despite the industry's legitimate concerns, there seems little likelihood that the initiative will be abandoned altogether. Law enforcement strongly backs it, and it is consistent with the direction of international standards.

What can a financial institution do to get in front of this initiative? A good place to start would be to review its AML risk analysis. Does the firm have enough information about those who own and control its entity-type clients to be comfortable that it accurately understands the AML risk presented by that customer? What about the potentially riskiest client types from an AML point of view: private investment vehicles, trusts and foundations? Is the firm comfortable explaining to regulators the choices it has made about the extent of the identification information it has gathered about these customers?

This is also a good time for financial institutions to review due diligence protocols for entity-type clients. Do procedures adequately take into account the individuals who own and control the entity, or are they focused exclusively on the entity itself? Chances are that background checks on a British Virgin Islands company or a Lichtenstein foundation are not turning up much that will be helpful in identifying and mitigating AML risk. To find out whether the people behind those entities have a criminal, regulatory, or other noteworthy past, a firm must perform checks on those individuals as well as on the entities themselves.

The firm's due diligence procedures should be reasonably designed to identify risk-relevant information that is readily available in the public domain. Moreover, riskier clients should receive a more thorough diligence review. Many firms check client names against a single database for negative news. Companies that have a range of client types from a variety of jurisdictions should consider whether it would be appropriate to expand the resources they use to search for

potentially negative information for at least some of their clients. They should also review whether the extent of the diligence they perform on their riskier clients genuinely deserves to be called "enhanced," or whether further measures are necessary to get the information they need for client selection and for fashioning controls to mitigate their AML risk adequately.

Once the relationship is initiated with the client, a financial institution's diligence obligations are not at an end. In this area, firms should also consider a risk-based approach to the frequency with which diligence checks are refreshed. Circumstances may change so that a client who appeared to present a low AML risk when the relationship began may later be revealed to present a higher risk. Companies that have procedures to identify which clients' risk profiles should be considered will be in the best position to take appropriate steps to mitigate the increased risk and thereby avoid problems before they happen. In addition, periodically checking for adverse media on existing clients can be an effective aid in meeting obligations to identify and report suspicious activity. It is appropriate to give particular attention to the transactions of clients who have become the focus of regulatory or law enforcement scrutiny. While employees may often spot adverse media coverage of existing clients, counting on them to do so may leave the firm unprotected.

Obtaining additional information about those who own and control entity-type clients will entail extra effort and expense. The same is true for performing robust diligence on riskier customers and keeping diligence on existing clients up to date. Firms seeking to protect themselves from negative headlines and other consequences of doing business with a client who uses a financial institution to commit financial crimes, will find that taking these steps is a prudent investment.



**Nikki Kowalski** is a Managing Director and Head of Kroll's Anti-Money Laundering Compliance Practice in New York. She is an expert in anti-money laundering laws and regulations applicable to financial institutions in the U.S. and other countries.

# CANADA OVERVIEW



Once again, this year's survey paints a positive fraud picture for Canada compared to the rest of the world: the overall prevalence dropped much more quickly than elsewhere so that fewer than half of businesses were hit in the past year and, on average, Canadian firms lost just 0.6% of revenues to fraudsters.



	2011-2012	2010-2011
<b>Prevalence:</b> Companies affected by fraud	47%	70%
<b>Areas of Frequent Loss:</b> Percentage of firms reporting loss to this type of fraud	Theft of physical assets or stock (24%) Management conflict of interest (14%)	Information theft, loss or attack (22%) Theft of physical assets or stock (16%)
<b>Areas of Vulnerability:</b> Percentage of firms considering themselves moderately or highly vulnerable	Information theft, loss or attack (28%) Theft of physical assets or stock (28%) IP theft (23%)	Information theft, loss, or attack (47%) Theft of physical assets or stock (34%) IP theft (35%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	58%	78%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	IT complexity (31%)	IT complexity (33%)
<b>Loss:</b> Average percentage of revenue lost to fraud	0.6%	0.9%

The data also reveal, however, a number of issues to which Canadian firms should pay attention. The first is that, amid the general decline, three specific frauds increased in frequency: theft of physical assets (from 16% of companies affected to 24%), management conflict of interest (from 13% to 14%) and regulatory or compliance breach (from 11% to 13%). For each of these, the prevalence in Canada is now at or above the global average. However, for all of these frauds, the levels of perceived vulnerability have dropped.

At the same time, Canadian respondents are among the most likely in the world to report that growing collaboration between firms is increasing exposure to fraud (21%). They are also less likely than average to be planning to invest in partner due diligence measures (33% compared to 38% for all companies).

It would be wrong to overestimate the fraud challenge faced by Canadian companies, but even in such a positive environment there are areas worth watching.

# Due diligence is essential and can be more time and cost efficient than you think



By Jennie Chan, Deborah Gold and Peter McFarlane

**Axioms become established because they are rooted in fact. “An ounce of prevention is worth a pound of cure” reflects the importance of taking thoughtful, effective precautions before embarking on a course of action and warns of the consequences of not doing so. In Canada, Kroll has recently seen numerous unfortunate outcomes attributable, in part, to the failure of individuals, corporations, or investors to obtain sufficient data to make an informed decision about a proposed transaction or investment.**

One recent case in particular illustrates the risk of inadequate vendor due diligence. A Canadian company was looking for a consulting firm to advise on procurement policies and controls, and to assist in reorganizing the purchasing department. The operational location was remote and only a limited number of candidates were identified. One firm had recently entered the Canadian market, had impressive credentials and presented well in interviews. The company felt fortunate to have the opportunity to work with such a well-qualified firm, especially as the reorganization needed to begin soon. The consulting firm was hired. No background checks were performed. The consulting firm hit the ground running, changing vendors on key supply contracts; running a tight ship – which, in reality, meant consolidating decision-making and approvals under their control; and aggressively responding to challenges or questions from within the organization. Ultimately, senior management realized there was a problem. A subsequent internal investigation revealed multiple

abuses by the procurement consultants, including false and inflated invoicing through related vendors and false expense reports. A search of public records also revealed allegations of fraud against this firm in another jurisdiction. A proper vendor background check would likely have identified these issues and avoided the substantial costs and reputational damage suffered by the company.

If the benefits of due diligence inquiries are so obvious, why do so many organizations fail to conduct adequate ones – or any at all – in preparation for key operational decisions? Over the years, we have heard many rationalizations for this behavior. Some are so common – and apparently so effective at undermining the importance of due diligence – that they have even made it to our Top Ten list [see box]. In certain instances, incentive structures – for closing a deal quickly or signing a large client – also work to discourage frequently time-consuming due diligence checks. Finally, the Global Fraud Survey consistently demonstrates that the primary fraud risk for companies is from

## The Top Ten Excuses for Poor Due Diligence

Make sure that, when faced with a situation that could have been avoided by appropriate due diligence, you are not relying on one of the following to explain things to investors and auditors.

1. Cost: "The quote for due diligence was significant and management wouldn't approve the expenditure." In our experience, such short term gain is likely to create long term pain.
2. Time constraints: "We needed to close the deal quickly." Fraudsters often seek to create a false sense of urgency in order to pressure victims into making quick decisions.
3. Volume: "We have thousands of vendors and third party relationships. It is simply not practical to screen them all." Techniques exist to focus due diligence resources effectively and thereby facilitate high-volume screening.
4. Low risk: "It was only a minor IT outsourcing contract. How much damage could a vendor in that position do?" A lot!
5. Sufficient existing controls: "We already have strong and effective internal controls –including segregation of duties and other checks and balances – that will stop, or at least detect, problem vendors." Typical internal control systems may not be adequate to detect reputational issues such as incidents of prior unethical conduct or connections to high-risk individuals and entities.
6. Reliance on third parties: "It's a well-known vendor in the industry. How would we have known that no one ever vetted them?" Never assume someone else did your due diligence for you.
7. Competition: "If we had insisted on conducting due diligence procedures, we would have lost the opportunity to a competitor who was willing to move ahead without such procedures." These are tough judgment calls for management. The risk of proceeding without due diligence should be fully assessed, but a competitor with poor risk judgment may not last long.
8. Relationship concerns: "We have to work alongside these people after the deal closes. They will think we don't trust them. My gut instinct tells me these are good guys." In an acquisition, the purchasing management is often reluctant to conduct intrusive background checks on the principals of the company being acquired. Gut instinct, though, has a long history of fallibility.
9. Reliance on referral source: "The fraudster was recommended by somebody I've always trusted," an advisor, friend, or family member. Earl Jones, Canada's Bernie Madoff, was meticulous in mining the relationships of his existing clients and his community to generate new victims to keep his fraudulent scheme afloat.
10. Exclusivity: "It felt like being on the inside of something big." This was the strategy used by Bernie Madoff. By creating an illusion of exclusivity, clients felt privileged to be able to place funds with him and disinclined to ask questions.

within: unethical employees are unlikely to engage in due diligence that would reveal their own misdeeds.

Although they are no reasons to ignore the need for due diligence, the appropriate cost and extent of such activity are legitimate concerns for any organization. In responding to them, a good first step is to understand the company's obligations, such as regulatory or contractual requirements to screen vendors, business partners, or clients under, for example, securities, anti-money laundering, or anti-corruption legislation. These represent the absolute minimum requirements for many companies' due diligence protocols.

The next step is to conduct a risk assessment of the organization in order to identify the level of risk associated with the various internal and external stakeholders involved with the business, which will inform the development of a framework for the level of due diligence required. To help with such assessments, many firms offer risk algorithms that assist in determining the level of due diligence necessary for the type of subject being investigated. This leads to a more time and cost effective approach because rather than all subjects undergoing the same process, more resources and greater attention are focused on the higher risk subjects. For a risk-

based approach to be effective, though, it is important to have protocols which determine what constitutes a red flag, the actions to be taken to address each concern and, ultimately, the organization's acceptance criteria.

Another consideration in designing efficient due diligence protocols involves identifying internal or external parties that require the organization to conduct investigations – and the extent of these requirements – in order to meet these obligations and to be able to report appropriate findings to each stakeholder.

Finally, technology should be leveraged. For organizations conducting a high volume of vendor or client investigations, it may be possible to automate a significant portion of the due diligence process, which can reduce costs and improve turnaround time. This includes the use of web-based portals to off-load the compilation of the subject's data.

In our experience, there is a growing acceptance of the need for adequate due diligence. Vendors want to be associated with well run, reputable companies and understand that vetting is now a best practice. In some instances, vendors will even pay for their investigation. Effective financial and reputational due diligence is standard operating procedure for most transactions. Organizations that do not utilize adequate due diligence protocols are vulnerable. One trait all successful fraudsters have is the ability to identify and exploit vulnerabilities. If those have been minimized, fraudsters will move on in search of easier targets.



**Jennie Chan** is a Managing Director in Kroll's Toronto office, specializing in complex financial investigations. Jennie has led and participated in a wide range of assignments, including internal fraud investigations, financial reviews and litigation support matters.

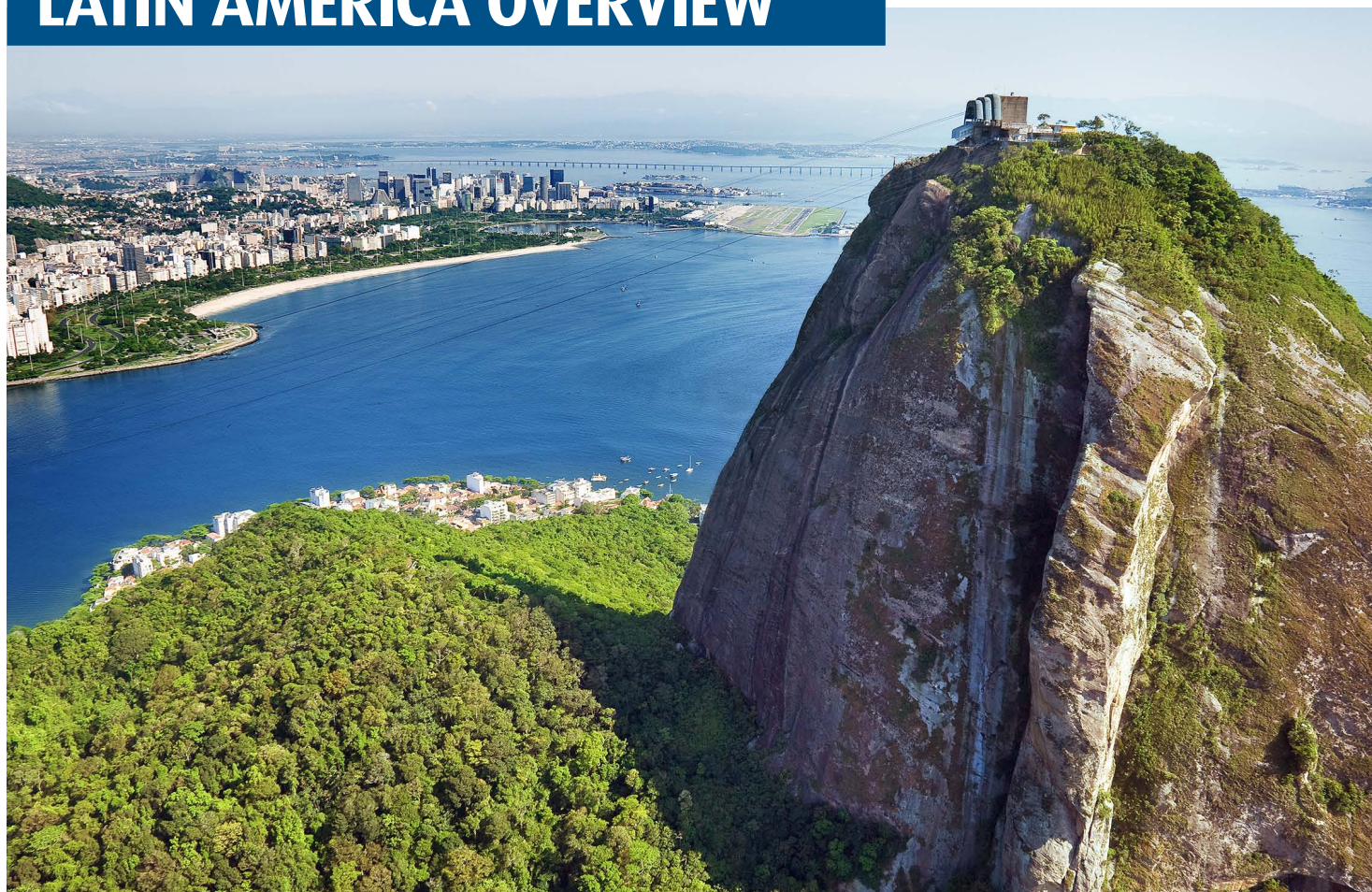


**Deborah Gold** is a Managing Director in Kroll's Toronto office. She provides due diligence solutions to support clients' commercial transactions, investments, and regulatory compliance requirements, and helps them manage legal, regulatory, financial, and reputational risk concerns.



**Peter McFarlane** is a Managing Director and head of the financial investigations team in Toronto. With more than 20 years of forensic accounting and investigative experience, Peter manages a wide range of complex financial investigations, litigation consulting, asset recovery and financial due diligence assignments for corporate and government clients around the world.

# LATIN AMERICA OVERVIEW



	2011-2012	2010-2011
<b>Prevalence:</b> Companies affected by fraud	56%	74%
<b>Areas of Frequent Loss:</b> Percentage of firms reporting loss to this type of fraud	Theft of physical assets or stock (19%) Information theft, loss or attack (16%) Vendor, supplier or procurement fraud (16%)	Theft of physical assets or stock (25%) Information theft, loss or attack (24%) Vendor, supplier or procurement fraud (23%) Corruption and bribery (23%) Management conflict of interest (21%) Internal financial fraud or theft (18%)
<b>Areas of Vulnerability:</b> Percentage of firms considering themselves moderately or highly vulnerable	Corruption and bribery (32%) Regulatory or compliance breach (32%) Vendor, supplier or procurement fraud (31%)	Corruption and bribery (70%) Theft of physical assets or stock (58%) Management conflict of interest (53%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	60%	79%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	IT complexity (21%) Entry into new, riskier markets (21%)	IT complexity (30%)
<b>Loss:</b> Average percentage of revenue lost to fraud	0.7%	1.9%

The good news is a relative thing in fraud. Latin America saw a marked drop in the prevalence of fraud overall and in most individual frauds in this year's survey compared to the last one. Looking beyond the changes, though, over half of companies suffered from at least one fraud in the last 12 months, including nearly one in five hit by theft of physical assets and one in six hit by information theft and vendor or procurement fraud. Just under a third of businesses admit to having moderate or high levels of vulnerability to corruption, regulatory or compliance breach, and vendor or procurement fraud. More worrying for the longer term, six in ten say that their exposure to fraud has increased.

A closer look shows more specific challenges at national levels: corruption and information theft in Mexico; vendor issues in Colombia; information theft, management conflict of interest, and the challenges of outward investment in Brazil. Because the intensity of these specific issues varies across the region, Latin American fraud this year is a study in contrasts. This makes the unique national challenges no less important for the companies and countries affected.

Fraud remains more the norm than the exception in Latin America. Efforts to fight it need to continue apace.

# Risk factors in Latin American agribusiness



By Andrés Otero

**The recent period of economic expansion in Latin America has been underpinned not only by the extraction of oil, minerals and other natural resources, but also by a booming agribusiness industry.**

Various Latin American countries have recognized that building their competitive advantage in agriculture is a path to economic development. It leads to the creation of new industries, generates skilled jobs and spurs innovation in science and technology. But developing a modern and efficient farming sector in Latin America requires significant investments in research, training, infrastructure, energy, irrigation and land acquisition. And these investments can be fraught with challenges and risks.

The financial crisis in Europe and the cooling of the Chinese economy will likely mean

lower prices for commodity producers in Latin America and a slowdown in foreign direct investment. Even so, it is important for Latin America to appreciate that its participation in the global economy cannot depend exclusively on oil and minerals. The region will need to draw upon its capacity to innovate and create value along the agricultural production chain in order to become a major global food supplier. Brazil and Chile, in particular, have already developed their agribusiness talents, but there are more opportunities to be seized across the region.

Brazil has long been the leader in agribusiness development in Latin America. By investing in research and development, Brazilian businesses have demonstrated that they can generate value along the food production chain. As a result, some of the world's top agribusiness firms have their primary operations in Brazil. Agribusiness companies have not only helped boost Brazil's GDP, but have also spurred the modernization and expansion of agriculture across Latin America. Opportunities in agribusiness now abound in Argentina, Colombia, Mexico, Peru, Chile and other countries in the region.

Beyond the broad macro-economic and political risks facing investors in Latin America, agribusiness companies must contend with challenges related to land ownership and title, the threat of social unrest, and the influence of organized crime, particularly the drug cartels in rural areas. Clearly, each country is different and poses its own set of challenges, but these are the principal risks that challenge potential investors – both foreign and domestic.

The issue of title ownership is particularly troubling in Latin America, where land conflicts have been a constant throughout much of the region's history. Many Latin American countries have undergone turbulent transformations from feudal farming systems controlled by a few privileged families to periods of violence and displacement under dictatorial regimes, guerilla occupations, drug cartel invasions and other forms of adverse land tenure, all of which contribute to the complexity of investing in agricultural lands.

Another important challenge is to understand the social tensions that exist in many rural areas. For the most part, Latin American countries have followed France's model of a centralized state structure, which resulted in governmental activities and the general population being concentrated in a few large cities. This model led to centuries of neglect in rural areas. The lack of basic infrastructure in many rural communities has created a potential time bomb of social unrest for many agribusiness investors, who are oftentimes faced with unresolved issues ignored by politicians for more than 200 years.

Also troubling is the presence of organized crime in the areas with some of the most fertile land in the region. Just as the best grapevines require fertile soil to prosper, so do the plants that produce illicit drugs.

As a result, drug cartels have sought to control large swaths of fertile land. Lands purchased by the cartels are often owned by front men or legally constituted entities in the service of the cartels. Entities doing business with these groups put themselves and their investments at risk of becoming a part of the process for laundering drug proceeds. Some ethanol and other biofuel production facilities in rural areas of Colombia, for example, have feedstock that originates from land controlled by drug cartels. Conducting business that directly or indirectly involves drug cartels poses no shortage of legal, reputational and operational risks for companies.

At Kroll, we have assisted a number of agribusiness companies in analyzing risks related to land ownership, organized crime and social tensions prior to investing. The reputational due diligence work we perform is not a substitute for the legal analysis of land titles, but rather complements this process. Through extensive searches of public records, interviews, site visits and development of local sources, we can

uncover red flags that reveal the risks to which our clients may be exposed through an acquisition or investment.

A thorough review of these kinds of transactions should be based on prudence and due diligence to allow investors to make informed decisions. A detailed investigation will help investors evaluate the opportunity, negotiate the price, develop a business plan, select the best partners, vendors and managers, and prepare them for regulatory or legal challenges that might arise, such as class action suits from local interest groups reclaiming their rights to the land.

Agriculture and agribusiness in Latin America present great opportunities, but also risks. One must first understand those risks in order to mitigate them.



**Andrés Otero** is a Managing Director and Market Leader for Kroll in Latin America. Andrés is an expert in a variety of investigative and intelligence areas, including fraud and anti-corruption services, money laundering investigations and conflict resolution matters.

## ECONOMIST INTELLIGENCE UNIT REPORT CARD

## NATURAL RESOURCES

The natural resources sector is another in which the news is mixed. Fifty-seven percent of companies in this sector (lower than the survey average) suffered at least one incidence of fraud, and losses due to fraud declined to 1% of revenues. On the other hand, information theft saw a modest rise in prevalence (from 22% to 25%) as did management conflict of interest (from 18% to 21%), with regulatory breaches remaining the same at 16%. Indeed, the sector had the second highest prevalence of any industry for the last two crimes as well as for theft of physical assets (30%) and market collusion (5%). The level of information theft is a particular concern because in this industry it involves far more than a compliance risk. Of those companies affected by such an attack this year, 43% had financial plans or data stolen. Fraudsters looking for such information present a threat to the company itself. Only 52% of natural resources firms, though, intend to invest in greater IT protection, a little below the survey average (53%).

**Loss:** Average percentage of revenue lost to fraud: 1%

**Prevalence:** Companies affected by fraud: 57%

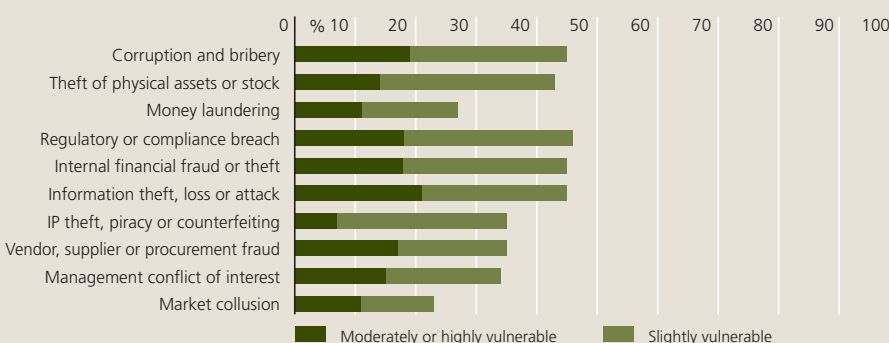
**Areas of Frequent Loss:** Percentage of firms reporting loss to this type of fraud

Theft of physical assets or stock (30%) • Information theft, loss or attack (25%)

Management conflict of interest (21%) • Regulatory or compliance breach (16%)

**Increase in Exposure:** Companies where exposure to fraud has increased: 57%

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



# BRAZIL OVERVIEW



Over half of Brazilian companies (54%) were hit by fraud in the last 12 months and, for the second year in a row, management conflict of interest was the most widespread problem. Nearly a quarter (23%) of the country's businesses reported an incident of this crime in the last year, well above the global average (14%) and the highest figure for this fraud for any country or region covered in the survey outside of Africa. Brazilian companies are also the only ones to report that, when there has been a fraud in the last year and the culprit was known, senior managers were just as likely as junior employees to be involved (each were key perpetrators 21% of the time). Brazilians recognize the problem: 29% of respondents describe their companies as moderately or highly vulnerable to management conflict of interest.

	2011-2012	2010-2011
<b>Prevalence:</b> Companies affected by fraud	54%	73%
<b>Areas of Frequent Loss:</b> Percentage of firms reporting loss to this type of fraud	Management conflict of interest (23%) Theft of physical assets or stock (17%) Information theft, loss or attack (14%)	Management conflict of interest (27%) Vendor, supplier, or procurement fraud (24%) Theft of physical assets or stock (16%)
<b>Areas of Vulnerability:</b> Percentage of firms considering themselves moderately or highly vulnerable	Information theft, loss or attack (31%) Management conflict of interest (29%) Vendor, supplier, or procurement fraud (23%) Internal financial fraud (23%)	Corruption and bribery (57%) Management conflict of interest (57%) Theft of physical assets or stock (49%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	74%	80%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	Entry into new, riskier markets (34%)	IT complexity (29%)
<b>Loss:</b> Average percentage of revenue lost to fraud	0.5%	1.8%

Nevertheless, only 51% of businesses plan to invest in more effective management controls, a figure not far above the survey average (46%). Moreover, 23% of companies report an increase in fraud exposure in the last year due to a weakening in internal controls – among the highest figures globally for this problem.

Another issue for Brazilian companies is addressing the fraud risk that inevitably arises out of their own globalization efforts: 34% report that entry into new, riskier markets is the leading driver of increased exposure to fraud, and an additional 17% say the same about increased collaboration with other firms in partnerships, joint ventures, and outsourcing. Similarly, concerns about fraud in other countries dissuaded 40% of Brazilian firms from investing in at least one foreign opportunity, with the risks of corruption, information theft, and market collusion being equally large concerns. Over half (51%) are investing more in due diligence in the next year – well above the survey average (38%) – but as more firms internationalize further this number may need to increase.



# The case for strengthening internal controls

By Vander Giordano

**In recent years, the Brazilian government has issued a series of regulations aimed at reducing the occurrence of financial fraud and tightening accounting standards. At the same time, Brazilian government agencies have been closely monitoring large corporations, both foreign and domestic. As a result, companies in Brazil have started to place a greater emphasis on regulatory compliance. Many are also making concerted efforts to foster a culture of ethical behavior among their employees.**

This homegrown vigilance against fraud is coupled with growing international observance of anti-corruption legislation. According to the Global Fraud Survey, 55% of companies say that their top managers, suppliers and overseas employees have received training to become both familiar and compliant with the Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act (UKBA). This is up from 43% from last year's survey. Nevertheless, despite the domestic and international pressures to comply with sound business practices, incidences of corruption continue to emerge, forcing banks and multinational companies to put more emphasis on internal controls.

The purpose of internal controls goes well beyond minimizing the risk of corruption. Internal controls are employed to reduce a broad spectrum of operational risks. These controls are divided into two basic categories: accounting controls and administrative controls. Accounting controls are procedures designed to verify that financial statements and other financial records accurately reflect the reality of the business. Operational controls, on the other hand, are procedures designed to monitor company activities, such as purchasing, inventory management, payments and production quality.

The following considerations relate exclusively to operational controls. Here are some of the key issues to consider when developing, implementing and calibrating operational controls: 1) the environment within which internal controls are developed; 2) the data that is produced as a result of these controls and the internal communication and utilization of such data; 3) the process of risk assessment and remediation within the company; 4) procedures for continued monitoring; and 5) risks to which the company is exposed. These considerations apply to companies in any industry, although each industry will have its own particular characteristics. We will illustrate each of these issues with a real case example.

**1. Control Environment** – Just as important as internal controls themselves is the process for developing the controls and the environment in which they are created. As a first step, producing a detailed flowchart to understand how data about procurement, sales, inventory, production quality and other operations move within the company can be very helpful. It is equally important to have a clear understanding of the management systems that process the data, such as the company's Enterprise Resource Planning

(ERP) systems and the security policies that are in place to protect that data.

## **Example: Database hacked at a communications company.**

A communications firm discovered that its database had been hacked. Our investigation indicated that, while the proper processes were in place, the security firewall was weak, lacking a number of standard features to detect and thwart intrusion. As a result, the perpetrator of the fraud was able to insert false information in the client database by using a sniffer that roamed the server undetected on a daily basis. We recommended that the password system be upgraded and that analytical software be added to monitor the activity on the system, which would alert the company when usage exceeded the norm or when any unauthorized users were detected.

**2. Information and Internal Communication** – The quality and reliability of the data that a company generates for management reports are fundamental to a company's decision-making process. Data that is not protected can be altered and lead companies in the wrong direction. It is essential that internal communication channels maintain the integrity of the data that is produced.

**Example: Data loss at a large service firm.**

A human resources consulting firm lost data when its database was migrated from one system to another. This case did not involve deliberate fraud but resulted in the miscalculation of employee benefits and ultimately, a number of incorrect payments. Our investigators recommended changes in the way in which employee pay stubs were distributed, implementation of procedures to review benefits calculations before the payments were issued, as well as changes in the password access and approval process.

**3. Risk Assessment** – It is important to be able to identify, fully understand, and accurately measure the risks to which a company is exposed. That means mapping out the company's operations and investments in controls. Once the primary risks have been identified, crisis response plans need to be developed and individuals must be assigned and trained to implement these plans in the event that problems arise.

**Example: Inventory depletion at a major manufacturer.**

A machinery manufacturer discovered an abnormally high rate of depletion in its stock of parts. Kroll's investigation revealed that nightshift employees had been forging signatures on service orders for parts that were not required. We recommended that all unused materials, as well as all used parts, be submitted at the end of each shift and then checked by the following shift. We also recommended the use of handheld computers for ordering parts from the warehouse, as well as an update of the signature manifest for employees authorized to order parts.

**4. Monitoring Activities** – The constantly changing environment in which a company operates requires continued renewal and updating of systems. It is important to develop tools to monitor company operations, such as procurement, inventory, production quality and payments and to maintain tight controls. The audit department should have a primary role in this monitoring process.

**Example: Credit limit breach at an investment bank.**

At an investment bank, a bank officer's portfolio had exceeded certain investment limits. Kroll compared the bank's historical investment activities to those of the individual officer. We discovered that the officer had committed fraud by using colleagues' passwords to alter the categorization of investments in various

portfolios. The fraud was detected by analyzing the bank's ERP, as well as by interviewing bank colleagues and clients. We recommended that the bank's monitoring system be focused on individual officers rather than on individual portfolios. In addition, we recommended installing a system to detect red flags in the ERP, upgrading the due diligence conducted in the assessment process for investments above a certain threshold, and an enhancement of auditing procedures.

**5. Risk Exposure** – Quantify and prioritize the risk to which the company is exposed. It is essential that the CEO and the CFO participate in this process. The company's strategic plan should include considerations of short-term and medium-term risks. Contingency plans should also be developed.

**Example: Corruption at a construction firm.**

A construction company employee responsible for business development was found by company auditors to have close ties to

government officials. Certain procedures involving new contracts with government agencies and officials had been concealed and the company suspected corruption. Kroll discovered that the lack of controls in the accounts payable department and in the supplier registry allowed the employee to process payments to a registered supplier without the supplier having provided any corresponding service to the company. An analysis of service orders, work assignments and manager approvals over a two-year period revealed these improper payments. Based on Kroll's recommendations, the company changed its supplier registration system, developed better password protections and strengthened its compliance program.



**Vander Giordano** is a Managing Director based in Kroll's São Paulo office. Vander has extensive experience working with companies in the energy, retail, banking and airline industries. He is a member of the Brazilian and International Bar Associations and holds an MBA.

**ECONOMIST INTELLIGENCE UNIT REPORT CARD****MANUFACTURING**

The manufacturing sector stands out in this year's survey—and not in a good way. Companies in this sector saw a substantial increase in the incidence of fraud, with 87% affected. Moreover, eight of the 10 frauds tracked for this survey became more common this year. The industry also experienced the highest levels of theft of physical assets (50%), corruption and bribery (29%), management conflict of interest (27%), vendor or procurement fraud (23%) and IP theft (13%). Finally, manufacturers experienced the highest average loss due to fraud in the survey (1.9% of revenue), and the sector was the only one to see this figure rise from last year. And future prospects are not bright either. Nine out of 10 companies believe their exposure to fraud increased over the past 12 months—yet another survey high. Despite this, companies are not addressing the problem. Over the past year, they were more likely than any other to weaken internal controls due to cost-cutting measures (31% did) and for almost every anti-fraud strategy covered in the survey, a substantially smaller number than average plan to invest in the next 12 months.

**Loss:** Average percentage of revenue lost to fraud: 1.9%

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

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

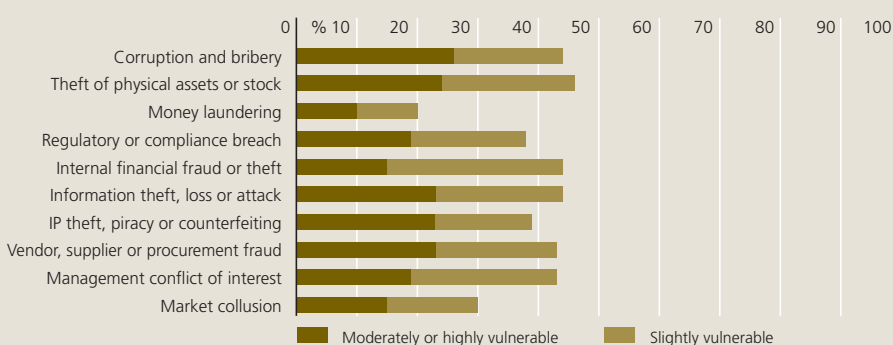
Theft of physical assets or stock (50%) • Corruption and bribery (29%)

Management conflict of interest (27%) • Vendor, supplier or procurement fraud (23%)

Internal financial fraud or theft (23%) • Information theft, loss or attack (21%)

**Increase in Exposure:** Companies where exposure to fraud has increased: 90%

**Biggest Drivers of Increased Exposure:** Most widespread factor leading to greater fraud exposure and percentage of firms affected: IT complexity (44%)



# MEXICO OVERVIEW



Mexico, in line with the rest of world, saw a reduced prevalence of fraud in the last year. Here, the most substantial decline was in the area of corruption and bribery (affecting just 15% of companies in the last 12 months compared to 37% the previous year). This improvement, however, is due to hard work rather than any substantially decreased risk.

	2011-2012	2010-2011
<b>Prevalence:</b> Companies affected by fraud	59%	69%
<b>Areas of Frequent Loss:</b> Percentage of firms reporting loss to this type of fraud	Information theft, loss or attack (26%) Theft of physical assets or stock (19%) Vendor, supplier or procurement fraud (19%) Corruption and bribery (15%)	Corruption and bribery (37%) Theft of physical assets or stock (31%) Information theft, loss, or attack (27%) Internal financial fraud or theft (23%) Vendor, supplier or procurement fraud (21%) Management conflict of interest (21%)
<b>Areas of Vulnerability:</b> Percentage of firms considering themselves moderately or highly vulnerable	Corruption and bribery (48%) Vendor, supplier or procurement fraud (44%) Regulatory or compliance breach (44%)	Corruption and bribery (81%) Theft of physical assets or stock (65%) Information theft, loss, or attack (58%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	56%	82%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	High staff turnover (22%) Weaker internal controls (22%)	IT Complexity (35%)
<b>Loss:</b> Average percentage of revenue lost to fraud	0.7%	2.2%

Fully 81% of companies have trained their senior managers, vendors, and foreign employees in FCPA and UK Bribery Act compliance, a level equaled nowhere else in the world except in Britain. Nevertheless, 48% of companies still say that they are moderately or highly vulnerable to corruption, the highest figure in the world after India's. Furthermore, the actual prevalence, however much improved from last year, is still markedly above the global average (11%). Maintaining this year's results will therefore take continued efforts.

Meanwhile, information theft has become the most widespread fraud in Mexico, hitting 26% of businesses – again above the survey average (21%). Companies, though, appear to be paying less attention to this crime. Only 22% – fewer than actually suffered from such theft in the last year – believe that they are moderately or highly vulnerable to it, and only 30% plan to invest in further IT protection in the next 12 months. The latter figure is markedly below the global average (53%) and the lowest for any geography covered in the survey.

Finally, procurement fraud remains a significant problem. It affected 19% of Mexican companies last year – well above the worldwide average of 12%. Following corruption, it is the fraud to which most companies feel moderately or highly vulnerable. Problems with fraudulent vendors are also exacerbating the issue of information theft: respondents report that when they suffered from the latter last year, 38% of the time vendor malfeasance was involved.



# Mexico's anti-money laundering challenges

By Ernesto Carrasco

**Most economists agree that Mexico has the potential to displace Brazil as Latin America's leading economic power. In order to fulfill this prophecy, Mexico faces daunting security challenges related to organized crime. First among them is reducing the rate of violent crime, which not only affects average Mexican citizens but, at the same time, sows uncertainty among foreign investors.**

During his six-year term, outgoing president Felipe Calderon implemented a military strategy against organized crime that achieved significant results in terms of combating the drug cartels, disrupting their operations and arresting high-profile leaders. In the process, security became the number one priority across the country. However, in terms of the economic impact of organized crime, Mexico has been less successful when it comes to implementing legal measures to deal systematically, both in the public and private spheres, with the related scourge of money laundering.

Mexico's money laundering problem is huge. According to the US Department of State, 95% of all illegal drugs sold in the US pass through Central America or Mexico. Mexico's Office of the Attorney General estimates that in 2012 some \$10 billion in drug trade proceeds were laundered within the country. It is little wonder that the Mexican drug cartels are among the wealthiest and most powerful in the world.

The 2012-2013 Global Competitiveness Report issued by the World Economic Forum warns that the primary factors undermining Mexico's economic growth prospects are corruption, organized crime, government bureaucracy and the lack of trust in country's police forces.

In mid-2012 a report released by the US Senate led to charges against London-based

HSBC bank that it had moved \$7 billion in cash from its Mexico unit to its US affiliate between 2007 and 2008 without investigating the origin of the money and failing to follow anti-money laundering procedures. Scandals such as this one are a clear signal that something is seriously wrong and that Mexican authorities need to sound the alarm. The \$27.5 million fine that HSBC was forced to pay to Mexican regulators for non-compliance with anti-money laundering regulations was widely criticized as a slap on the wrist.

Between January 2007 and July 2012, only 83 individuals were convicted of money laundering in Mexico, a tiny number given the size and extent of the problem. This disappointing result is symptomatic of the larger problem. Mexico clearly needs to develop tougher legal measures pertaining to anti-money laundering in order to confront criminal organizations that are fueled by drug money, which would include legal reforms to facilitate the confiscation of assets of suspected criminals and of third parties suspected of assisting such criminals in their laundering of money. Experience in Colombia shows that one of the most effective tactics against organized crime is to hit these criminals where it hurts most – in their wallets.

Mexico's private sector can also play a role in combating money laundering. It can do this by promoting a culture that respects the country's laws and their consequences, a business ethic based on internal controls that include, among other things, preventative measures to vet suppliers and other third parties in supply chains, rigorous due diligence on clients and business partners, and limits on cash payments for purchases of all kinds, but especially big-ticket items, such as cars and real estate.

In Mexico, the clandestine business operations of the drug cartels have permeated the entire economy, even state-controlled areas such as the oil industry. Government authorities have credible information that not only is organized crime involved in the illegal trade of stolen gasoline, but also that legally constituted businesses are among the most habitual buyers in this illicit trade.

Real estate and construction are two other sectors that are awash with cash, because buying homes, buildings and land with cash is one of the easiest options for organized crime to launder money. The result has been rapidly rising real estate prices. This bubble,

when it bursts, will have a negative impact on the whole economy.

If Mexico really wants to become a regional economic leader, the government will have to lay the groundwork. That means pushing through reforms that modernize the public sector, promoting transparency in business and helping reduce corruption of government officials.

Colombia can be a useful guide, in terms of approaches that were successfully employed, and also identifying the ineffective measures so that they are not repeated. Some of the most important lessons to be learned from Colombia are based on the political will to push through institutional reforms that allowed the country to confront the drug cartels. These included strengthening the judicial system, providing the police with better training, taking tough actions against corrupt public officials, especially high-level officials, and implementing legal measures to confiscate assets derived from criminal activities. These and other actions, such as increased collaboration between business leaders and government officials, as well as mobilizing civic groups to protest against violent crime, have helped Colombia turn the tide against the cartels.

Among the negative experiences in Colombia's fight against anti-money laundering that should be highlighted is the idea of negotiating with criminal organizations when they have the upper hand. In Colombia's case, this was a strategic blunder. Colombian history shows that it is first necessary to weaken organized crime before opening negotiations. And that means not just arresting cartel leaders, but also confiscating their assets.

The international community is waiting to see if Mexico is up to the task. If concrete measures, including anti-money laundering and national security laws that have been pending for months in Congress, are adopted soon, this will help generate confidence among foreign and domestic investors. If such measures are not adopted, not only may Mexico miss the chance to become an economic leader in the hemisphere, but it may also be branded as a high-risk country that is increasingly off-limits to foreign investment.

**Ernesto Carrasco** is Managing Director and Head of Kroll's Mexico office. He is a lawyer by profession, with an extensive career in the public and private sectors in Colombia, leading investigations related to organized crime, corporate investigations and financial fraud.



# TOP EXECUTIVES

## A culture of fraud on the rise

By Matías Nahón

An infamous Argentine politician coined the expression “I steal for the Crown”, in an attempt to justify the corrupt practices of which he was accused.

In Argentina, the corruption that can permeate the corridors of power is not restricted to government. In the private sector, Kroll’s experience shows that fraud and corrupt practices have steadily risen among top executives in recent years.

An analysis of the financial damages caused by acts of fraud within companies reveals that those committed by mid-level and top management account for more than 85% of losses, according to a nation-wide survey published in 2011.

As severe as they may be, the financial damages are only part of the story. The reputational costs caused by fraud may be even higher. Companies that fall victim to fraud can suffer a debilitating crisis of confidence, both among its employees and its clients, which may take much time and effort to overcome.

In Kroll’s investigative experience, fraud committed by top management in Argentina often goes undetected for a long time, even when employees not directly involved in the fraud were aware that the fraud was occurring at an early stage. Interviews conducted by Kroll in connection with these

investigations have repeatedly revealed that low and medium-level employees fail to report fraud for fear of being fired if they step forward, and only do so when the fraud becomes blatantly obvious or outrageous.

While 72% of companies in the Global Fraud Survey indicated that they have well-developed whistleblower programs, Argentine companies are lagging in this area and need to do more to reassure employees that they will be protected if they report abuses.

Kroll’s investigations indicate that the great majority of fraud cases involving top executives in Argentina come to light as a result of anonymous reports by current or former employees, and not as a result of internal audits or comprehensive controls that have been implemented by senior management. Developing whistleblower programs would likely go a long way toward uncovering fraud at an earlier stage, and thereby potentially saving them from significant financial and reputational damage.

The ways in which large-scale fraud is committed are similar when they involve local firms that have been acquired by multinational firms or investment funds that are not intimately familiar with the local business environment. Multinationals often choose not to change an acquired company’s management based on the reasoning “if it works, don’t fix it”. However, problems can eventually arise due to the lack of oversight controls. In many cases, the internal audit

department in these local firms either does not exist or is not adequately trained and equipped to detect fraud. To make matters worse, external audit firms in Argentina explicitly declare that they have no mandate to either detect or thwart internal fraud, when auditing a client. This is a recipe for impunity, conducive to irregularities of all kinds.

One of the most common fraudulent practices carried out by top management is the hiring of outside suppliers, which are owned by friends or relatives, and which supply services or products only to that one client. In addition to the obvious conflict of interest from overlapping loyalties, the services or products provided are frequently of sub-standard quality. The damage to the company caused by this double whammy can be severe, although often difficult to precisely quantify, based on Kroll’s investigation of a variety of fraud cases in this area.

Another common fraudulent practice is using company assets for personal benefit, or contracting the company’s suppliers to perform personal favors. Although this type of fraud generally does not have high financial impact to the organization, when discovered they generate a negative image for the company, and set a bad example for employees. There is little incentive for rank-and-file employees to treat company property with respect, work hard or behave with integrity, when they observe their superiors profiting at the firm’s expense.

Yet another form of fraud perpetrated by top management is the manipulation of local financial statements submitted to (sometimes distant) headquarters offices. Motives for this type of fraud vary. For example, top executives may want to conceal embarrassing losses, or boost profitability levels in order to trigger desired bonus payments.

We have only seen a handful of Argentine companies invest in fraud prevention. In situations where little attention is given to prevention, and lack of attention is compounded by a general lack of internal controls, it is no surprise that fraudulent acts by disloyal employees frequently lead to severe losses for Argentine companies.



**Matías Nahón** is an Associate Managing Director and Head of Kroll’s Buenos Aires office. Matías manages a wide variety of complex assignments, including investigations into fraud, due diligence, litigation support and asset searches.

# COLOMBIA OVERVIEW



Colombian respondents report a lower than average fraud prevalence in the last year – only 49% were affected by at least one fraud in the last 12 months compared to 61% globally – but their other answers in the survey indicate that this may have involved at least some element of luck.

	2011-2012*
<b>Prevalence:</b> Companies affected by fraud	49%
<b>Areas of Frequent Loss:</b> Percentage of firms reporting loss to this type of fraud	Vendor, supplier, or procurement fraud (19%) Theft of physical assets or stock (19%) Regulatory or compliance breach (14%)
<b>Areas of Vulnerability:</b> Percentage of firms considering themselves moderately or highly vulnerable	Corruption and bribery (30%) Theft of physical assets or stock (30%) Regulatory or compliance breach (30%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	46%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	IT complexity (24%)
<b>Loss:</b> Average percentage of revenue lost to fraud	0.4%


\*Insufficient respondents in 2011 to provide comparative data.

Thirty percent, for example, report being moderately or highly vulnerable to corruption, theft of physical assets, and compliance breach – all above the survey average – and for other frauds they report vulnerability levels at or near the global norms.

One of the biggest problems in Colombia in the last year has been vendor or procurement fraud, affecting 19% of companies. This figure is well above the survey average of 12% and ties with that of Mexico for the highest level for any country or region other than India. Accordingly, where companies have suffered a fraud and the perpetrators are known, one third of companies report the involvement of vendors in the last year, compared to 17% for the survey as a whole. However, only 32% of Colombian companies say that they will be investing in partner or vendor due diligence in the next 12 months, well below the survey average (38%).

Colombian respondents see information theft as a looming threat: 27% believe that they are already moderately or highly vulnerable to this crime and the most prevalent driver of increased fraud exposure in the country is growing IT complexity (cited by 24%). Here, though, companies appear ready to take action: 76% intend to invest in greater IT security in the next year.

Colombians know that this year's reported fraud levels do not reflect the underlying risks. Informed decision-making can help address them better.



# Vendor and procurement fraud in Colombia

By Recaredo Romero

**Vendor and procurement fraud, along with regulatory non-compliance, is the most common type of fraud impacting companies in Colombia. According to Colombian executives who participated in this year's Global Fraud Survey, 19% of Colombian companies experienced this type of fraud, which was significantly above the global average (12%). Vendor and procurement fraud is of particular concern, not only because it is so widespread, but also it can result in such high financial impact – among the highest of all types of fraud. It is essential for companies to understand and mitigate the risks associated with vendors and the procurement process.**

Vendor and procurement fraud comes in many shapes and sizes: kickbacks, bid rigging, phantom vendors, product switches, collusion among vendors and the fractioning of orders to stay below certain purchase limits (and, thereby, below the radar of internal controls). In cases of vendor and procurement fraud, the perpetrator can be a vendor or a company employee or, in most cases, a supplier and an employee working in concert. These frauds, which involve a vendor collaborating with a company insider, are often the most difficult schemes to detect.

## **No company is immune**

In Colombia, procurement fraud affects companies in every industry. No organization is immune. However, the risk of exposure to procurement fraud and the required

measures to mitigate that risk vary from case to case. The oil and mining sector, for example, which has been a big factor in fueling economic growth in Colombia in recent years, is particularly vulnerable to this kind of illicit behavior.

Of the \$13.2 billion of foreign direct investment that flowed into Colombia in 2011, more than 80% was destined for the oil and mining sector. The investments required for oil and mining exploration and production are large and involve the hiring of hundreds or even thousands of suppliers of goods and services. Such vendors often have standards of professional behavior and ethics that differ from the companies contracting them. Unfortunately, the rapid growth of the oil and mining sector is not always accompanied by similarly robust development of internal controls. To make matters worse, fraud is a dynamic phenomenon, which requires companies to constantly review, adjust and strengthen their internal controls.

In our experience, vendor and procurement fraud in Colombia most often involves employees in management positions, who use their authority to undermine or manipulate the internal controls pertaining to the vendor hiring and negotiation process. These insiders often enjoy a high level of prestige within the organization and are seen as dedicated and hard-working individuals. Department and business unit heads, project managers and other senior employees with influence over the acquisitions process usually fall within this definition. The level of confidence that top management has in these often high-performing employees can sometimes lead to more relaxed supervision of their work, more willingness to accept excuses given for irregularities, breaches of procedures, and failure to identify red flags. A procurement committee, an internal control mechanism for avoiding these situations, is a key line of defense that needs to be constantly reinforced.

### Who controls the procurement committee?

Vendor and procurement fraud has been uncovered in many of the cases that Kroll has investigated in Colombia over the past 12 months. In several cases, fraud was detected in the procurement process after vendor proposals had been evaluated and selected by the procurement committee. Establishing a committee to oversee purchases above a certain amount is a practice that is widely accepted in Colombia as an effective measure of internal control. In several cases, however,

the procurement committee proved to be anything but effective.

A common factor in these cases was a high level of technical complexity in the products and services being procured, and the fact that very few if any members of the procurement committee had sufficient technical knowledge to adequately evaluate the competing proposals. These same committee members were often either directly or indirectly responsible for identifying eligible vendors and sending them invitations to bid. This kind of undue influence over the procurement process can lead, in extreme cases, to the selection of the highest-cost proposal based on an argument of superior quality or experience of that particular vendor.

In these cases, what we discovered was a procurement committee that was being held hostage, in effect, by one of its members, who exercised an excessive degree of influence over the purchasing decisions. When faced with this situation, it is important for the company to undertake a thorough review and address the weaknesses identified. This might lead to changing the composition of the committee or to hiring an outside firm to provide an independent evaluation of vendor proposals.

### Prevention and detection

When it comes to vendor and procurement fraud, the emphasis should always be on prevention. This requires that companies dedicate efforts and resources proportional to their level of exposure to the risk of fraud. It is important for companies to have tools at their disposal that allow them to detect fraud at an early stage and, in the event that fraud is detected, to ensure that its impact is minimized and that it is not repeated. There are a broad range of prevention and detection measures. Here are three that warrant special attention:

#### » *Know your employees and your vendors:*

While this may seem like an obvious precaution, conducting due diligence on vendors or employees that wield influence over purchasing decisions is too often not done, or done with insufficient rigor. Many cases of fraud that Kroll has investigated in Colombia could have been prevented if the organizations had conducted the proper due diligence. Due diligence needs to be taken seriously. It cannot be treated as a tick-the-box exercise. Furthermore, companies should do periodic follow-up background checks on vendors and

employees, even after vendors have been selected and employees hired, to ensure that information is up to date.

- » *High-tech tools for data analysis:* Today, most companies capture a lot of electronic data. Utilizing this data through data mining and advanced analytics can be an effective tool for preventing or detecting fraud. By using mathematical models and applying a variety of tests, vast quantities of valuable data can be probed and analyzed for red flags that might otherwise go undetected. These may include particular patterns in the procurement process, unusually fast growth in sales to certain vendors or other deviations from the norm.
- » *Whistleblower procedures:* Warnings from employees and vendors is the most common method of fraud detection. Tip-offs are especially important when it comes to fraud that is particularly difficult to detect, as is frequently the case with procurement fraud. It is essential to open channels that facilitate confidential reporting of questionable or illicit behavior within the organization. This year's Global Fraud Survey reflects the rapid adoption of whistleblower procedures by companies around the world; 72% of companies said they had a whistleblower process in place. In Colombia, all of the executives who participated in the survey indicated that their companies had established such procedures, which was far from the case five years ago. This is a significant advance. However, establishing whistleblower procedures is only half the battle. It is important that the implementation of the whistleblower procedures, and the response from the company when reports are made, produce a high level of confidence in the system and thereby provide an incentive for employees and vendors to use it effectively and, in the process, generate a positive outcome for the company.

Vendor and procurement fraud can have a significant financial impact on a company. It can also lead to reputational damage that is difficult and costly to repair. It is important to be proactive and never to dismiss or underestimate any red flags that may appear.

**Recaredo Romero** is a Managing Director and Head of Kroll's Bogota office. He manages a wide variety of complex assignments, including major fraud investigations, Foreign Corrupt Practices Act compliance, business intelligence, litigation support, asset recovery and due diligence matters.

# CHINA OVERVIEW



China's fraud landscape has improved significantly in the last 12 months, showing a considerable drop in overall prevalence compared to last year. However, the data also suggest that a very worrying complacency may be developing.

Even after recent improvements, the number of companies hit by at least one type of fraud (65%) is still higher than the global average (61%). Moreover, the incidence of certain individual frauds, notably theft of physical assets (27%) and corruption (19%), either rose or stayed the same.

Corruption in the country is not only as widespread as last year, it is also still well above the global average (11%). In addition, for companies hit by a fraud in the last 12 months where the perpetrator was known, a government official or regulator played a leading role in 26% of cases. Nevertheless, the survey revealed that attention to corruption has diminished at too many companies: only 19% of respondents said that they were moderately or highly vulnerable to it, compared to 64% last year.

IP theft presents a similar picture. Although the number of Chinese companies reporting an incident of this fraud was just 8%, this was still slightly above the global average. However, only 10% of companies believe that they are even moderately vulnerable to a loss of IP, less than half the figure for this year's survey as a whole (21%) and down sharply from 54% last year. Moreover, the number of companies planning to invest in IP protection in the coming 12 months (29%) is substantially lower than the survey average (43%). IP protection has seen undeniable progress in recent years in China, but the battle is certainly far from won.

As Chinese companies expand globally, a lack of focus on the attendant fraud risks could also prove dangerous: 40% of Chinese respondents reported that entry into new, riskier markets is the leading driver to increased fraud exposure at their companies – one of the highest figures globally. On the other hand, the danger of fraud dissuaded only 8% of Chinese firms from investing in a foreign location in the past year, less than a third of the survey average (27%). Chinese companies should be more mindful of the local fraud threats when entering risky markets.

	2011-2012	2010-2011
<b>Prevalence:</b> Companies affected by fraud	65%	84%
<b>Areas of Frequent Loss:</b> Percentage of firms reporting loss to this type of fraud	Theft of physical assets or stock (27%) Information theft, loss or attack (21%) Corruption and bribery (19%)	Vendor, supplier or procurement fraud (33%) Information theft, loss or attack (28%) Management conflict of interest (23%) Internal financial fraud or theft (20%) Theft of physical assets or stock (20%) Corruption and bribery (19%)
<b>Areas of Vulnerability:</b> Percentage of firms considering themselves moderately or highly vulnerable	Regulatory or compliance breach (40%) Internal financial fraud (33%) Information theft, loss or attack (29%)	Corruption and bribery (64%) Information theft, loss or attack (56%) Vendor, supplier or procurement fraud (55%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	69%	84%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	Entry into new, riskier markets (40%)	High staff turnover (43%)
<b>Loss:</b> Average percentage of revenue lost to fraud	0.8%	2.3%



# Proving staff kickback allegations: How to gather evidence efficiently

**It is not uncommon for a company to receive a warning that an employee in its procurement department is receiving favors from a supplier, which results in the company paying above market price. We see such allegations of vendor kickbacks – undisclosed payments by vendors directly to their clients' employees in exchange for preferential treatment – more than you might expect.**

By Penelope Lepeudry and Abigail Cheadle

This year's Global Fraud Survey found that nearly one in eight companies suffered from vendor, supplier, or procurement fraud in the last year alone. In places like India or Mexico, the risk of this type of fraud is even greater – in these regions, the proportion reaches about one in five. The size of the consumer goods and manufacturing industries in these countries means that vendor kickbacks and fraud can translate into significant financial losses as a result of a lost, stolen or diverted inventory.

How do you find out whether there is any truth to the claim that an employee is receiving kickbacks from a supplier? Investigating kickback allegations is not easy, for many reasons:

- » Direct evidence of the transaction is not typically documented in the company's accounting books and payment records;
- » Suppliers' accounting books and records are not generally made available to their clients unless it is a key supplier or the contract includes a broad audit clause;
- » Large companies usually have hundreds, if not thousands, of vendors, so it is difficult to pinpoint which one(s) may be providing kickback payments;

» A vague allegation will not be investigated by law enforcement agencies so it is imperative to conduct an internal investigation to obtain sufficient evidence in order to make a compelling case.

Such investigations must be undertaken to stop financial leakage and to minimize exposure to the UK Bribery Act and other applicable anti-corruption legislation that imposes liability for receiving bribers in the private sector.

## Recommended procedures

To begin gathering evidence and building a case, companies should take the following steps. It all starts with notifying and obtaining advice from your in-house counsel on what is needed to get the investigation started, ranging from who takes the lead and the extent of the said parties' involvement in the investigation.

Next, secure potential evidence. The methods of doing so will vary based on how and where the data is stored. For electronic data, IT departments generally have neither the equipment nor the expertise to collect and secure evidence. For example, accessing the electronic data runs the risk of altering or deleting data, and if such data is altered, it may not be admissible. To make sure that anything collected will be admissible in court if needed, engage a computer forensics

expert if you do not have the in-house capabilities for data collection.

At a minimum, you should consider securing the following electronic data from the following sources by imaging them and setting them aside:

- » Email servers and email backup tapes;
- » Company mobile devices – done in conjunction with company policy and applicable law – of key suspects, such as procurement, finance, and general management staff (such devices include, but are not limited to, mobile phones, digital assistants, tablets, and similar equipment); and
- » Company laptops or other electronic equipment used by suspect employees.

Finally, any paper-based key procurement and contract data such as supporting invoices, receipts, bills, and delivery acknowledgements from the alleged perpetrator's tenure with the company need to be secured.

Once the relevant evidence is secured, an investigation into the allegation itself is required. If there is no in-house expertise to address this, the option would be to hire external consultants.

Data analysis of the company's financial records may shed light on vendors that have been favored since joining the company.

If there is a broad audit clause in place with your suppliers, this data analysis could expose and bring to light the approved supplier's transactional data. Suppliers willing to pay kickbacks, though, are unlikely to agree to the incorporation of such an audit provision in their agreement.

Finally, data analytics can help identify relevant statistics about vendors, such as the degree to which the amount of business they have been given has increased over a certain period of time. Significant increases indicate those most likely to have paid kickbacks. You will need to review transactions with such vendors thoroughly, including the bidding process, the award, the contractual arrangements, the unit prices and the quality of services or goods delivered. Data analysis is usually a very effective way of spotting inappropriately favored vendors.

Background searches on these vendors are often useful in obtaining information such as financial statements, ownership structure, litigation records, and overall reputation. Such searches on suspected employees may also be a valuable source of data.

If there is conclusive information pointing to an employee's involvement, an asset tracing exercise can be carried out as well. While only indicative, if the employee is found guilty, such information will be useful in any recovery actions.

You will also need to identify any vendors who have seen a significant decrease in business or have been removed from the vendor database during the alleged perpetrator's tenure with the company. These rejected vendors who have seen a drastic drop of their revenue at your company may have complaints regarding favoritism and biased procurement processes against the company's procurement ethics. They can be approached for informal discussions or interviews and discreet enquiries to find out why they are disgruntled. Frequently whistleblowers come from this pool.

More often than not, kickbacks are arranged through in-person meetings and the only evidence a company may find will be in emails, text messages, or calendars – both electronic and paper. This is why it is important to scrutinize the latter for suspicious meetings. Surveillance of these meetings, where legally permissible, can also provide pertinent information on the individuals involved.

Finally, desk and office searches often reveal modus operandi: the beneficiaries of bribes,

their amount and nature, and even where the money is kept. For example, a email will give you some information of the meeting being set up, a calendar invite could then reveal who was present at the meeting, payment records can confirm that an inadequate payment was made and background searches on the payment receiver could expose that the payment was given to a relative of a meeting attendee.

The combined analysis of paper and electronic data, procurement records, discreet enquiries with vendors (no longer being favored), and background searches will give you a good understanding of what, if anything, is going on and who might be involved.

Rather than relying only on investigations, because vendor kickbacks schemes are very difficult to detect, companies need to focus on mitigating the risk before it happens by implementing whistleblower initiatives not only for employees but also for vendors and customers; implementing an iron-clad

procurement process; having a strong tone at the top; regularly rotating procurement staff; and employing robust pre-employment screening policies.



**Abigail Cheadle** is a Managing Director in Kroll's Southeast Asia practice based in Singapore. Abigail has more than 19 years of experience across Asia, Australia, USA, Europe, and the Middle East, leading investigations into fraud, corruption (including alleged breaches of the FCPA), and accounting irregularities, as well as managing multi-jurisdiction asset-tracing projects.



**Penelope Lepeudry** is a Managing Director in Kroll's Southeast Asia practice based in Singapore. She has over 17 years of experience conducting financial investigations and internal audits across Europe, USA, and Asia. Penelope has conducted numerous FCPA investigations and compliance reviews, financial misstatement reviews, prepared expert witness reports for dispute resolutions, performed risk and internal audit reviews and led fraud prevention training for various organizations.

## ECONOMIST INTELLIGENCE UNIT REPORT CARD

## CONSUMER GOODS

Of all the companies surveyed, those in the consumer goods sector recorded the second lowest overall number of companies affected by fraud (51%) and the lowest average losses (0.4% of revenue). Moreover, not only did the prevalence of every fraud except regulatory breach decline, the figures for corruption and bribery (6%), IP theft (4%) and market collusion (1%) were the lowest in the survey. Amid these positive findings, two issues are still apparent. First, the sector had the second highest level of vendor or procurement fraud of any industry (18%). A below-average number of consumer goods firms are looking to invest in enhanced screening of partners and vendors (33% compared with 38% on average in other sectors). The other issue is a traditional one for the sector: the disappearance of companies' products and assets at the hands of staff, especially junior employees working for short durations. This year is no exception. The prevalence of the theft of physical stock declined only slightly in the past 12 months and two-thirds of businesses that suffered a fraud and knew the culprit reported that a junior employee was involved, the highest level for any industry. The sector recognises the problem: high staff turnover is again blamed as the biggest cause of increased fraud exposure. It is not tackling the issue aggressively, though. The number of companies planning to invest in staff background checks (42%) only slightly exceeds the average (41%), and nearly one in five (18%) companies are actually weakening the internal controls that can thwart fraud.

**Loss:** Average percentage of revenue lost to fraud: 0.4%

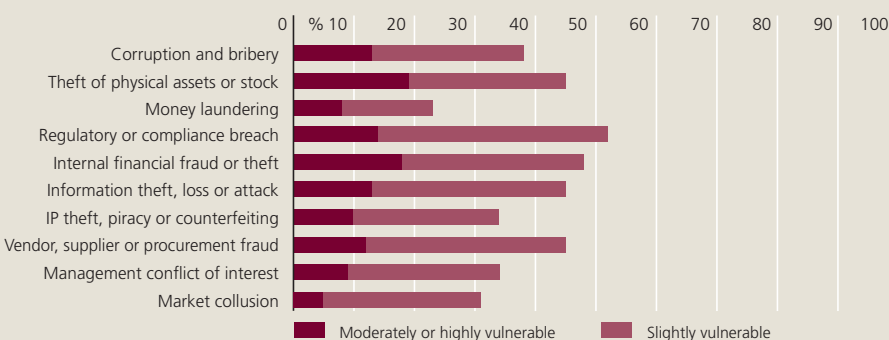
**Prevalence:** Companies affected by fraud: 51%

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

Theft of physical assets or stock (26%) • Vendor, supplier or procurement fraud (18%)

**Increase in Exposure:** Companies where exposure to fraud has increased: 57%

**Biggest Drivers of Increased Exposure:** Most widespread factor leading to greater fraud exposure and percentage of firms affected: High staff turnover (21%)





# Preventing IP fraud: The better option

By Sam Olsen

**According to a report commissioned by the International Chamber of Commerce, the total global economic value of counterfeit and pirated products, based on 2008 data, is as much as \$650 billion every year<sup>1</sup>. Given the natural opacity of intellectual property (IP) fraud, the US Patent and Trademark Office believe that the real figure could be substantially higher than this. With every single illegal product representing both lost company revenue and 2.5 million job losses in G20 countries alone, the effects on the bottom line should not be ignored.**

Traditionally, companies and institutions have tackled the theft of their intellectual property by trying to solve the problem after the theft has occurred. Much like insuring a building after it has burnt down, this approach has several flaws.

First, once a trade secret, patent, or any other IP has been stolen, it is highly likely to be out in the open forever. Even with the most fastidious clean-up operation, someone somewhere will still be able to take advantage of the leaked IP. Stories of businesses that did not monitor employee access to IT networks are common. We know of a recent example where several top engineers at a Western chemical company saved critical schematics of a reactor on a USB device before resigning en masse and walking out the front door unhindered. Within hours, these plans could have been in the hands of hundreds if not thousands of engineers and competitors around the world.

Second, the cost of addressing an IP theft problem can be huge. Although legal remedies are generally effective at inhibiting

the production and shipment of counterfeit products, especially in the United States, it can be surprisingly expensive to obtain an injunction. In America, for example, a company can seek relief under Section 337 in order to force a suspected infringer of its IP to cease and desist, or even to have it excluded from the United States market. Yet the cost of launching such a case can be very high, and with a separate action needed to claim damages, the complainant may not be able to recoup all of his losses and costs. Although the courts recently awarded Apple an eye-popping \$1 billion in its infringement case against Samsung, this is not necessarily representative.

Third, IP theft can markedly reduce revenue. Legal wrangling can sometimes lead to production being shut down while the case is being resolved, which may sometimes be a long drawn-out process. Meanwhile, as happened to a client of ours in East Asia recently, the company can find itself losing out to competitors going to market with products that have been generated from its own IP.



Resolving IP theft after the event, then, is not the most effective strategy. This year's Global Fraud Survey shows that 8% of companies were victims of IP infringement in the past year. Many, if not the majority, of these businesses have no real IP-theft protection plans in place, a pattern repeated across the world. Even in the United Kingdom, a country with an economy highly reliant on intellectual property, research has shown that some 40% of businesses take no practical action to protect their IP<sup>2</sup>.

Several simple measures can substantially reduce the risk of IP theft:

» **Third party screening:** Verifying that a company's employees are who they say they are, and that they do not have professional relationships with your competitors or have been involved with IP theft before, is a simple but often overlooked step in the hiring process. In a similar vein, background checks on potential vendors and partners can sometimes reveal interesting connections that might signal a risk to your IP. A large French IT company would have

prevented the loss of many of its new microchip designs if it had conducted some basic background checks on 'students' it was giving work experience to – many of whom were actually paid employees of a major competitor.

» **Physical security measures:** Putting in place comprehensive technical and operational physical security measures, policies, and procedures can dramatically enhance IP protection. Also, regular security audits of facilities and processes can give senior management reassurance that the measures are still effective or indicate where improvements can be made. One of Kroll's clients recently requested a compliance audit of IP security measures that had been installed in 2009 in one of its China facilities. Although most remained sound, the cleaners had recently been given full access to the whole site but had not undergone a background clearance first – a clear breach of best practices.

» **Information technology security measures:** Firewalls, external device policies, penetration testing – all of these

can significantly contribute to the defense against IP theft.

It is impossible to guarantee the safety of your intellectual property completely, but these simple precautions can reduce the risk. With even the US Patent and Trademark Office recognizing that IP crime is not a top priority for governments – they are generally much more concerned about drug, weapon and human trafficking – it is critical that companies enhance the security of their IP themselves. As with a virulent illness, prevention is always preferable to treatment.

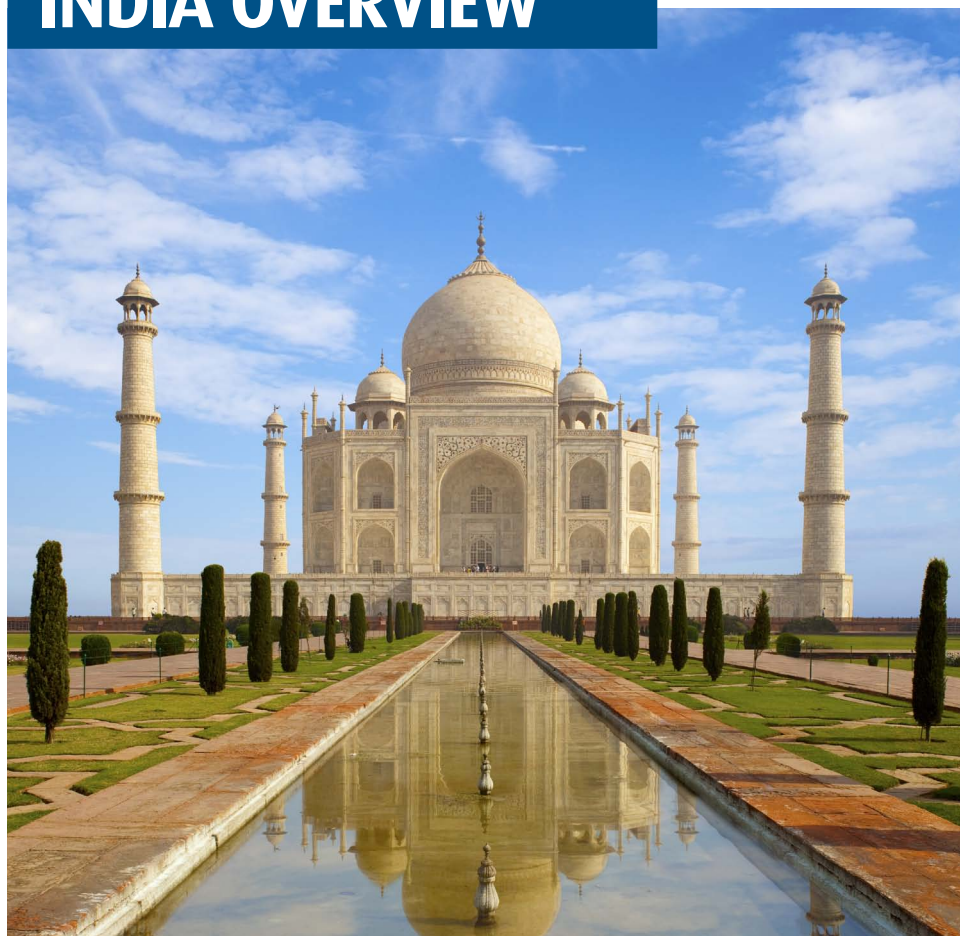


**Sam Olsen** is an Associate Vice President and Head of the Asia security practice. Sam is responsible for providing security services, which includes threat, risk and vulnerability assessments and physical security, to a wide variety of local and multinational companies throughout Asia.

<sup>1</sup> International Chamber of Commerce. Estimating the global economic and social impacts of counterfeiting and piracy, February 2011

<sup>2</sup> Alliance For Intellectual Property. "Impact of IP theft facts and figures". Accessed September 26, 2012, [http://www.allianceagainstiptheft.co.uk/facts\\_figures.html](http://www.allianceagainstiptheft.co.uk/facts_figures.html)

# INDIA OVERVIEW



**India, despite some improvements, remains a challenging fraud environment. Outside of Africa, it possesses the highest number of companies affected by fraud of any region or country (68%) and its average loss to fraud (1.2% of revenues) is significantly higher than the global average (0.9%).**

Moreover, eight of the 10 frauds covered in the survey were more widespread in India than they were globally, in particular: internal financial fraud (22% of Indian companies were affected compared to 12% overall) and vendor or procurement fraud (20% compared to 12%).

The number of firms affected by corruption dropped in the last year from 31% to 20%. Nevertheless, this is still well above the global average (11%) and corruption remains a leading fraud concern: half of Indian companies still report themselves moderately or highly vulnerable to it.

Indian respondents appreciate that they have a significant fraud risk: except for management conflict of interest, they are noticeably more likely than average to consider their companies moderately or highly vulnerable to every type of fraud covered in the survey. However, this does not automatically translate into addressing the problem. In the next year, Indians are less likely than average to be investing in eleven of the twelve anti-fraud strategies covered in the survey.

In particular, despite high levels of concern about information theft, only 40% plan to spend on IT security, compared to 53% globally. Moreover, in the last year, 22% of Indian firms have weakened their internal controls, frequently as a result of budget constraints. This is one of the highest figures for any country in the survey.

The survey brings to light the need for Indian companies to be more active in combatting fraud.

	2011-2012	2010-2011
<b>Prevalence:</b> Companies affected by fraud	68%	84%
<b>Areas of Frequent Loss:</b> Percentage of firms reporting loss to this type of fraud	Theft of physical assets or stock (27%) Information theft, loss or attack (23%) Internal financial fraud or theft (22%) Corruption and bribery (20%) Vendor, supplier or procurement fraud (20%)	Corruption and bribery (31%) Information theft, loss or attack (27%) Internal financial fraud or theft (23%) Theft of physical assets or stock (23%) Vendor, supplier or procurement fraud (22%) Management conflict of interest (19%)
<b>Areas of Vulnerability:</b> Percentage of firms considering themselves moderately or highly vulnerable	Corruption and bribery (50%) Information theft, loss or attack (37%) Theft of physical assets or stock (34%)	Corruption and bribery (78%) Vendor, supplier or procurement fraud (59%) Information theft, loss or attack (58%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	67%	85%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	IT complexity (43%)	High staff turnover (41%)
<b>Loss:</b> Average percentage of revenue lost to fraud	1.2%	2.2%



# Procurement fraud in India: Overcoming a widespread problem

By Reshmi Khurana

**Companies around the globe source raw and finished products from India, drawn by the country's relatively low labor costs. It is a major procurement center for several industries, notably textiles, home products, jewelry, fashion, and back office services. Corporate procurement strategies vary: some international companies have exclusive local purchasing offices; others buy from businesses that specialize in sourcing products for international companies; while others still send representatives directly from overseas offices to find the best suppliers of the goods they require.**

Regardless of the industry or the procurement policy, every company needs to be aware of the risk of procurement fraud in India. According to the recent Global Fraud Survey, the proportion of companies worldwide affected by vendor, supplier, or procurement fraud fell from 20% in 2011 to 12% in 2012. In India, however, the problem remains more widespread, with 20% of respondents from that country saying that they were affected by such fraud in the last 12 months, a figure little changed from the year before. Kroll's experience in investigating this type of fraud for international companies operating in India sheds light on the nature of the problem that these numbers reveal.

Apart from vendor kickbacks, the most common procurement-related fraud to which these companies have been subjected involved senior management conflicts of interest. In such cases, the managers of these foreign firms have a vested interest in private purchasing companies, as they are able to

obtain favorable rates and terms with manufacturers for their own self-run companies. In turn, these personal businesses are often suppliers for other local and international companies, as well as to the competition. The senior managers in question might employ family members and friends in the purchasing organization who will help conceal the conflicts. To make matters worse, such vendor fraud is often accompanied by information theft, including pricing, employee, and customer data.

In Kroll's experience, the most common driver of procurement fraud within international companies in India is the lack of familiarity with the local market. For companies which India is not a large market, this increases the exposure to procurement-related fraud. High staff turnover in the local Indian offices is a key driver of this type of fraud. It makes it difficult to build employee loyalty, and a culture of deference towards senior management serves as a disincentive for junior staff to report fraud. Finally, vendors of

international companies that pay kickbacks to managers are often unhappy, but do not complain about the ongoing fraud and corruption to the company's senior management for fear of losing the business. Sometimes, international companies sourcing in India have found senior managers from other overseas offices colluding with their India counterparts by also accepting kickbacks from vendors.

Procurement-related fraud often raises red flags, but companies do not always investigate them with the appropriate tools, such as forensic accounting, or they do not go far enough by making inquiries both inside and outside the organization. The red flags that might appear include: whistleblower complaints from employees or vendors; unusual turnover; unusual patterns in promoting or hiring staff; and the addition of new vendors to the supplier matrix without conducting sufficient due diligence. Companies that have experienced such fraud also usually have weak internal controls and reporting systems. For example, Enterprise Resource Planning systems often do not directly link the local sourcing organization with the headquarters. These businesses frequently have separate accounting systems for their local and home entities, which makes it difficult to implement checks and balances. This problem may even be getting worse: 22% of Indian businesses report increased fraud exposure due to a weakening of internal controls in the last year.

Companies that are least vulnerable to procurement fraud usually have good information security protocols in place. This controls and restricts data sharing that could potentially reduce the risk of access control systems being compromised. With a well-organized internal control system in place, which allows for due diligence on new employees and vendors, audits are more straightforward. Finally, firms that have an anonymous and independent whistleblowing system will benefit, as this encourages local employees and vendors to report unethical behavior and in turn, protects them from direct and indirect punitive actions.



**Reshmi Khurana** is an Associate Managing Director and Head of Kroll's Mumbai office. She has more than ten years of experience conducting pre-transaction due diligence on the management, operations and business models of organizations for M&A transactions ranging from \$20-30 billion. Her clients include asset management companies, corporations in the mining, oil & gas, consumer packaged goods and pharmaceutical industries and law firms.

# Challenges facing emerging market corporations expanding abroad



By Richard Dailly

As economic globalization has increased in depth and breadth, more corporates from emerging markets are now making their stamp on the international business community. Operating in numerous jurisdictions brings about risks from a lack of local knowledge, and companies face a pressing need to start building business relationships from scratch.

The Global Fraud Survey indicates that 15% of companies surveyed worldwide suffered an incident of management conflict of interest in the last year. Companies operating outside their native countries, often with country representatives or managers overseeing foreign operations, therefore need to take special care.

Some compliance risks vary widely depending on the company's internal business culture, business norms within the sector in which it operates, and the culture of its home country. Two of Asia's largest emerging markets, India and Indonesia, serve as a good example of how different the challenges they face can be.

## India

Many of India's major family-led corporations date back over decades and are now into their second or even third generation of leadership. Each new generation has brought enhanced professionalization of management. The country has also turned out an international class of trained managers, frequently educated in American or European universities.

This fine-tuned managerial capacity, combined with a lengthy presence in Western markets, has made Indian firms adept at working within stringent compliance regimes in the United States and Europe. They take their regulatory responsibilities seriously, including assiduous compliance with the likes of the Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act.

Corporate management in India may thus feel that its operations throughout the world are meeting their compliance requirements. However, Indian companies with a global presence now need to also pay particular attention to their compliance obligations in Africa, Southeast Asia and South America, which have become more stringent. This means considering the implications of the FCPA and UK Bribery Act wherever these companies operate.

In our survey, however, at least 25% of Indian companies, although subject to at least one of these laws, have not conducted an assessment, trained the right people, nor amended their due diligence processes accordingly. Management needs to be fully aware of the risks in less controlled markets and to ensure that proper controls and accountability are in place.

## Indonesia

The appetite of Indonesian companies for expansion abroad is a generation behind that

of India, but it is growing very quickly and with it the risk of fraud: 26% of Indonesian respondents to the Global Fraud Survey reported that entry into new, riskier markets was the leading cause of increased fraud exposure in the last year. The problem is especially acute for the country's extractive sector, which includes some of world's largest mining companies.

Currently, many Indonesian companies invest heavily in emerging markets such as Africa and elsewhere in Asia. Such companies with operations limited to Indonesia and these other emerging markets may still find themselves caught in the nets of both the FCPA and the UK Bribery Act, which can impose fines on individuals and companies. In addition to potential liability under the FCPA and UK Bribery Act, there may be applicable local anti-corruption legislation, which when enforced, can have a devastating effect.

A second possible issue for Indonesian companies investing in emerging markets, and particularly in the extractive sector, is the heightened focus worldwide over environmental issues, land rights and the movement of people. For instance, in these markets, it is not uncommon for

environmental licenses to be obtained through corrupt methods. If proper due process has not been followed, an innocent partner or investor may find that it does not have the rights to operate on land it is mining.

Similarly, in less developed markets, there are examples of indigenous people either being paid money to leave their homes, and if they refuse, being forcibly removed. Local officials directing gangs are frequently involved in unethical enforcement. If an investor or its affiliate finds itself linked to such activity, the cost can be significant not only in terms of fines and fees, but also in terms of the reputational damage, which can sometimes have an even more significant, longer-lasting impact.



**Richard Dailly** is a Managing Director based in Singapore responsible for high-level case management and business development in South and Southeast Asia. He has over 20 years of experience in global risk for the British government and Kroll Advisory Solutions. 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

## ECONOMIST INTELLIGENCE UNIT REPORT CARD

## RETAIL, WHOLESALE & DISTRIBUTION

According to the survey, the average overall prevalence of fraud is slightly lower than average for the retail, wholesale and distribution sector. Almost six companies in every ten in the sector report being hit by fraud at least once, although the average loss due to fraud was just 0.5%, the second lowest level of any sector. That said, retail's perennial problem— theft of physical assets or stock—remained relatively high (25%). The data reveal one notable peculiarity for the industry. The number of insiders—employees and agents—involved in frauds is about average (66%), but companies in this sector are the most likely to be hit by fraud involving customers (23%) and the third most likely to be targeted by vendors (24%). That suggests companies ought to be paying attention to their supply chains, but the survey finds that they are slightly less likely than average to be investing in partner, client and vendor due diligence (36% compared with 38% for the overall survey). More attention here could pay dividends.

**Loss:** Average percentage of revenue lost to fraud: 0.5%

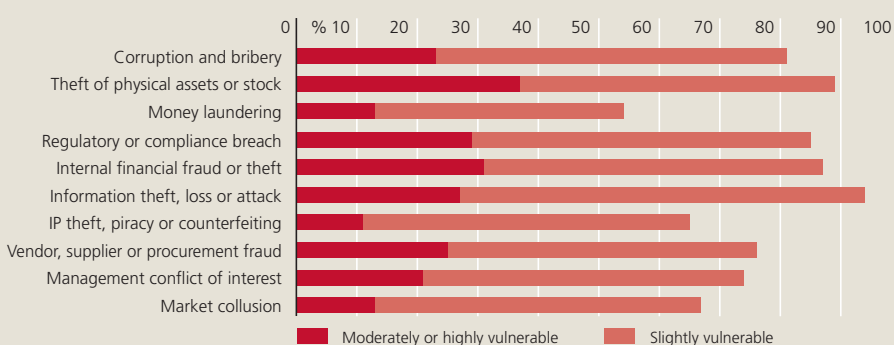
**Prevalence:** Companies affected by fraud: 58%

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

Theft of physical assets or stock (25%) • Information theft, loss or attack (15%)

**Increase in Exposure:** Companies where exposure to fraud has increased: 60%

**Biggest Drivers of Increased Exposure:** Most widespread factor leading to greater fraud exposure and percentage of firms affected: Entry into new, riskier markets (28%)



# INDONESIA OVERVIEW



Indonesian companies experienced a comparatively high overall incidence of fraud (65% were affected at least once in the last year, compared to 61% globally). Moreover, they have significant problems with information theft (at 35% the highest geographic figure in the survey, just greater than Africa's 34% and well above the global rate of 21%); regulatory and compliance breach (23% compared to just 11% overall); and internal financial fraud (19% compared to 12% worldwide).

The latter two frauds are also among the three threats to which Indonesian respondents feel most vulnerable.

Indonesian companies are prone to fraud from the inside: 82% of those firms which suffered one type of fraud and knew the perpetrator named an employee or an agent compared with 67% globally. Among insiders, agents are a notable problem, with 32% of affected Indonesian firms saying that one had played a significant role in a fraud in the last year, well above the global average of 18%.

Vendors are also more likely to engage fraud in Indonesian than they are elsewhere: 22% of affected companies report that a vendor played a leading role, compared to 17% worldwide. More striking, 33% of information theft – the country's biggest fraud problem – involved vendor or supplier misconduct, the highest figure globally and more than double the overall average (15%). This helps explain the country's above average level of vendor fraud (16%).

A new phase in globalization is also directly contributing to fraud risk for many Indonesian firms. Like its Asian counterparts, Indonesian companies are increasingly looking to move onto the global stage, in particular with investments in Asia and Africa. These activities bring great opportunities, but also fraud dangers. So far, Indonesian firms have been relatively conservative, with 35% putting off investment in at least one foreign market because of perceived fraud issues, compared to 27% globally. Nevertheless, entry into new, riskier markets is the leading driver of increased fraud, cited by more than a quarter of all Indonesian businesses (26%).

	2011-2012
<b>Prevalence:</b> Companies affected by fraud	65%
<b>Areas of Frequent Loss:</b> Percentage of firms reporting loss to this type of fraud	Information theft, loss or attack (35%) Regulatory or compliance breach (23%) Internal financial fraud or theft (19%) Theft of physical assets or stock (16%) Vendor, supplier or procurement fraud (16%)
<b>Areas of Vulnerability:</b> Percentage of firms considering themselves moderately or highly vulnerable	Corruption and bribery (33%) Internal financial fraud or theft (33%) Regulatory or compliance breach (30%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	63%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	Entry into new, riskier markets (26%)
<b>Loss:</b> Average percentage of revenue lost to fraud	0.6%

\*Insufficient respondents in 2011 to provide comparative data.



# Dealing with trade secret issues

By Kunio Sakaide

**In April 2012, a major Japanese steelmaker, Nippon Steel Corp (NSC), sued Posco, its South Korean partner, for \$1.2bn for allegedly stealing trade secrets in a move that highlighted the pressure on Japanese companies to protect their confidential information amidst intensifying global competition.**

NSC claimed that Posco used illicit means to obtain highly specialized technology developed by NSC to manufacture grain-oriented electrical steel sheets, used in power plant generators. NSC also sued a former NSC employee whom it claims was involved in Posco's alleged trade theft.

## **Trade secret...More than just the technical information**

Some companies choose not to register their intellectual property, namely, patents, designs, trademarks or copyrights. Instead of trying to maintain the confidentiality of such content by treating them as trade secrets, corporate trade secrets can sometimes be

classified into two generic types: technical information and management information. The former refers to the accumulated knowledge and technical expertise in product development and production. Generally, most companies tend to be more concerned about this kind of information. However, as the Global Fraud Survey results suggest, there is a wide range of different types of information that can be exploited by competitors depending on the nature of their objectives. In the professional services sector, 49% of thefts involved a search for financial or strategic data, while only 33% sought customer data. On the other hand, in the financial services sector, the figures were nearly identical – 46% and 50% respectively.

Management information at risk can be include business strategies, investment plans, procurement information, distribution routes, information on subcontractors, vendors and customers. Based on statistics above, companies should be more aware of fraud incidences like this from occurring.

### Routes of trade secret leakage and counter measures

Trade secret leaks can be attributed to many factors, ranging from disgruntled individuals, business partners, competitors, criminal organizations and even state organizations. However, in many cases, trade secrets are leaked via current or former employee, during product distribution processes (photos and videos), in documents, or electronic data. The mass retirement of the baby boomer generation in Japan has impacted companies in a variety of different ways, such as accelerated corporate restructuring, transfers of factories and research and development functions to overseas locations. Other contributing factors include the shrinking of the domestic market, the devaluation of the Yen and the rapid mobilization of human resources. Information technology has also played a part as its evolution has allowed for information leakage to be done more covertly, with the advent of smaller memory devices to facilitate these practices.

In Japan, many companies have already established a certain level of security measures, including periodic inventory checks, identification and classification of trade secrets, as well as the establishment of access control systems both from an IT security and a physical security perspective. Companies use access control systems to limit access rights only to authorized users and this prevents unauthorized access to the companies' trade secrets. However, even at companies with these measures in place, classification of different security levels and implementation of security management protocols are often left to the judgment of managers operating in different departments or units, and as a result, there is a lack of consistent, company-wide information management systems (including back-office departments, such as legal).

In order to achieve these standards, it is recommended to conduct background screening on employees who are granted access to confidential information or secure systems. Additionally, companies should securely preserve the electronic data of retired employees as it may provide valuable information, should the company need to conduct a detailed follow-up investigation on the employee's activities during the time in which they were employed.

### Internal Investigation

When information leakage occurs, it is critical for companies to thoroughly investigate the incident in order to accurately identify the source of this breach. The investigation can also provide a good opportunity to identify vulnerabilities in the company's information management system. However, in reality, many companies tend to close the investigation at a rather early stage by citing insufficient funding, the lack of human resources and the constraints of time. They often request their employees who committed information leakage/theft to voluntarily resign from the company, and in some cases, even offer them payment severance package or retirement benefits. Though there may be times when these measures work well, they are risky in that they can negatively affect remaining employees' motivation or loyalty to the company, due to the company's "soft" approach to the incident.

### Protecting Business Partners' Information

Companies are increasingly facing the need to implement effective security measures to manage partners' information as well as their

own. In recent years, through participation in joint ventures, business alliances and mergers and acquisitions, companies are increasingly given opportunities to access and handle their business partners' sensitive information. Given the current business market dynamics, this trend is likely to continue. Companies tend to be less careful with regards to the handling of another companies' information (even if they are business partners), and there is a greater risk of information leakage or possible misuse of shared information, which can result in a deterioration of business relationships. It is also important for companies to request their partners to securely manage shared information, as well as to establish a system that enables both parties to constantly monitor each other's control level.



**Kunio Sakaide** is an Associate Managing Director with Kroll in Tokyo, specializing in due diligence, conducting internal investigations, corporate security, and facility security consulting services. Kunio has managed numerous complex due diligence, business intelligence, and fraud investigation cases and has assisted clients in the litigation and recovery process.

## ECONOMIST INTELLIGENCE UNIT REPORT CARD

## PROFESSIONAL SERVICES

Typically in past surveys, the professional services sector has performed well in terms of avoiding fraud compared with others. This year is different. Although there has been some improvement since last year—notably a drop in the number of companies that believe their exposure to fraud has increased and in the average losses due to fraud—the results are mixed. This is one of just two industries that saw an increase in the number of companies affected by fraud in the past year. Seven of the 10 frauds tracked in the survey actually rose in prevalence in the sector, most notably the theft of physical assets (28% of firms were affected this year compared with 15% last year) and information theft (32% were affected this year, up from 23% last year). The latter should be a particular concern for the industry: professional services companies saw the highest occurrence of information theft of any industry and were the second most likely to say that IT complexity was the leading driver of increased fraud exposure (41%).

**Prevalence:** Average percentage of revenue lost to fraud: 1.2%

**Prevalence:** Companies affected by fraud: 68%

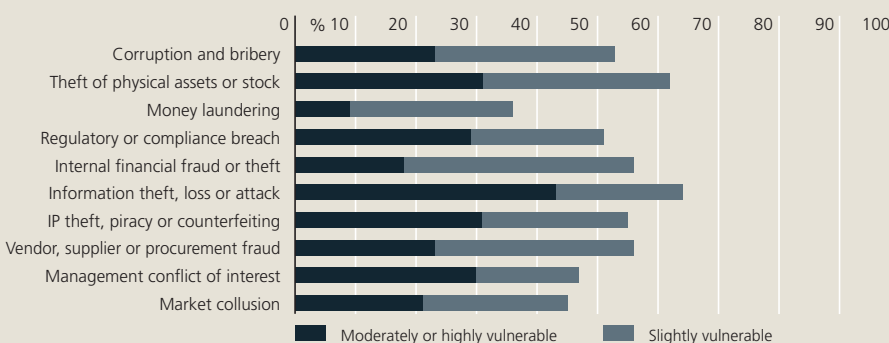
**Areas of Frequent Loss:** Percentage of firms reporting loss to this type of fraud:

Information theft, loss or attack (32%) • Theft of physical assets or stock (28%)

Management conflict of interest (16%) • Vendor, supplier or procurement fraud (16%)

**Increase in Exposure:** Companies where exposure to fraud has increased: 72%

**Biggest Drivers of Increased Exposure:** Most widespread factor leading to greater fraud exposure and percentage of firms affected: IT complexity (41%)



# EUROPE OVERVIEW



The rest of the world's fraud figures have improved faster than Europe's, so that operating on the continent now represents an average rather than a low fraud risk. The number of companies affected by at least one fraud (63%) is slightly higher than the global average (61%) and, for seven of the ten frauds covered by the survey, the European incidence is within one percentage point of the overall figure.

	2011-2012	2010-2011
<b>Prevalence:</b> Companies affected by fraud	63%	71%
<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 (18%)	Theft of physical assets or stock (23%) Management conflict of interest (19%) Information theft, loss or attack (18%) Internal financial fraud (16%) Vendor, supplier or procurement fraud (14%)
<b>Areas of Vulnerability:</b> Percentage of firms considering themselves moderately or highly vulnerable	Theft of physical assets or stock (26%) Information theft, loss or attack (23%) Regulatory or compliance breach (23%)	Information theft, loss or attack (47%) Theft of physical assets or stock (41%) Management conflict of interest (39%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	56%	74%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	IT complexity (27%)	IT complexity (33%)
<b>Loss:</b> Average percentage of revenue lost to fraud	0.8%	2.0%

Furthermore, the continent's two most common frauds, theft of physical assets (23%) and information theft (18%), have remained at a fairly constant level for the last three years

European companies are, for many types of fraud, less likely to see themselves as in danger – a possible sign of complacency. For example, for internal financial fraud, only 20% of Europeans consider their businesses moderately or highly vulnerable, compared to 26% worldwide, and for IP theft the equivalent figures are 17% and 21%. In both cases, however, the actual incidence of these frauds was higher for European respondents than for the survey as a whole. Similarly, except for physical asset protection, Europeans are less likely to be planning to invest in every anti-fraud strategy covered by the survey than are their counterparts worldwide. For IP theft, the European figure is 35% but the global one 43%.

Such investment, though, yields results, as European efforts on corruption show. The survey indicates that the number of the continent's companies which have formally assessed the risks associated with the UK Bribery Act and US FCPA has more than doubled within the last 12 months, as has the number providing relevant training for employees and agents. The incidence of corruption, meanwhile, fell from 14% last year in Europe to 10%. Having controls in place may also have opened up global investment. Last year, 28% of all European companies were dissuaded from investing somewhere in the world because of the danger of corruption. This year it was down to 9%.



# Bank collapses amidst mismanagement & fraud

By Brendan Hawthorne

Bank collapses have been both a cause and a symptom of today's economic malaise, with government and depositor losses running into trillions of dollars. Where is this money now and why did the banks crash? Owners, management, compliance departments, regulators, and even governments are all in the frame. Investigators charged with looking into bank failures must keep uppermost in their minds the suspicion that the institution has been the victim of fraud, possibly perpetrated by the highest levels of its management.

When a bank collapses, the inquest should start with an examination of the loan book. Its construction, the lending decisions, and the approach to loan management it reveals may answer why the institution was left exposed to unsustainable losses. From here,

mismanagement can be differentiated from fraud and abuse.

This part of the investigation may uncover malpractice by bank owners and managers. For many, the temptation to misuse funds is too great. They may think that no one will

know if they help themselves or friends to depositors' money through loans made on a cozy basis, sometimes even bearing no interest; they may even believe that the funds will eventually be repaid. The truth, though, can quickly become clear when a bank is in financial difficulty and people want their money out immediately. The chances that those who borrowed the cash will then have it to return are remote.

"Insider lending" is more frequent in emerging markets where bank owners have lent to groups of relatives or to members of the country's elite. This practice may result from lack of control, or even naiveté, in handling and building the loan book. By lending to a cluster of inside parties, the bank may simply have wanted to cement its position at the hub of the country's economy. When the global economy went into reverse, however, it exposed just how risky the practice was.

A loan book investigation may also unearth abuse by borrowers. Some will use the bonds of friendship to deceive bankers into giving a loan, or claim to be better placed to repay the money than they actually are. Many fraudsters also piggyback one loan on another, giving a false impression of their net worth. When struggling banks sought repayment, these individuals were shown to have acted fraudulently. By then, however, the money was lost.

Analysis of the loan book is most challenging when both the owner or manager and external borrowers engage in fraud. They may pillage the bank by colluding in the arrangement of loans, using disguised or fabricated documentation to circumvent credit allocation committees and internal controls. Some banks became little more than Ponzi schemes, with growth in depositors' money used to keep the institution afloat after fraudulent borrowers had ceased to service their loans. In such situations, the risks of funds going missing, and of failure itself, are the most severe.

Although fraud can bring down a bank, it is not the only cause of a collapse. Another cause is irresponsible lending, such as what took place during the mid-2000s. Then, bankers regarded loan making as a source of quick, easy fees and profits. They wanted their deposits out in the market place to capture demand and buoyant asset prices.

Many may have been advised by more cautious colleagues to avoid some business, but the opportunities looked endless and almost nobody wanted to miss them. Property in the Gulf States, for example, looked like an exciting investment for high rollers during the early part of the last decade but, when prices collapsed, returns bit the dust. The fortunes of many banks also plummeted as a result of the Dubai property melt-down; some needed bailouts.

Rash lending was also evident in developed markets such as the United Kingdom. While there is no suggestion that criminality was involved, when the bubble burst in 2008, the value of assets built up by companies like Royal Bank of Scotland, HBOS, and Bradford and Bingley collapsed. They too were forced to take multi-billion pound government bailouts.

From issuance of overly risky loans in Britain to insider lending in emerging markets, these asset price collapses exposed banks, as customers lost faith in their solvency and opted to withdraw their funds. Those without lenders of last resort – and their deposit guarantee schemes – could not survive without the funding and failed.

The process of dissecting the loan books of these banks was painful. It exposed breaches of a multitude of banking rules. Contracts and other documentation were severely flawed as bankers rushed to do deals; decisions were taken without proper due diligence; collateral valuations were weak or non-existent. Wherever you looked, fee-making had driven executives and prudence was nowhere to be found. At the very moment when compliance was most needed, it was ignored by deal-makers addled by the adrenalin of the boom.

It has taken some time for the worst excesses to be exposed, although the loss of control was evident in virtually every aspect of banks' activities during this period. Several instances of alleged rogue traders have appeared in the last couple of years, following on from the discovery of Jérôme Kerviel, the rogue trader who lost Société Générale \$4.9 billion in 2008. A similar alleged flouting of good compliance practice was exposed this year with the Libor rate fixing scandal. Banking fraud – once a relatively neglected subject –

has now been brought to the front of the public consciousness. Bankers have taken the blame for the recession.

These losses have given regulators a license to act tough. American regulators, for example, have imposed heavy fines on a number of financial institutions for issues such as lax anti-money laundering systems and OFAC breaches. Britain's Financial Services Authority (FSA) imposed its heaviest ever fine this year for Libor manipulation and European regulators are investigating further such cases. The continued investigation of banking systems by regulators is likely to produce new allegations, revelations, and even more charges.

Regulators are under pressure to clamp down on bad practice. Banks have no option but to cooperate with their requests and admit to errors. Compliance has become a top priority in the boardroom, even if that means that the bank takes a less aggressive posture in the

market and has to lower its return on capital. Basel III rules on capital adequacy have stopped any attempt to revert to aggressive lending.

Whether the modernized, less aggressive banks are also stronger ones is a matter for speculation. For now, banks are more likely to be picking up the pieces from a period when many either collapsed or came uncomfortably close to doing so. The wisest ones are building up compliance systems and anti-fraud techniques to ensure that the worst excesses will never be repeated, and are pro-actively investigating questionable past practices in a bid to manage the reputational fallout from further regulatory probes.



**Brendan Hawthorne** is a Managing Director and Head of Kroll's Dubai office. He has 17 years' experience in forensic and financial investigations. Brendan has worked on many large and high profile investigations with a primary focus on financial institutions, managing complex international frauds, multi-jurisdiction asset-tracing and large accounting investigations

#### ECONOMIST INTELLIGENCE UNIT REPORT CARD

#### FINANCIAL SERVICES

This year respondents reported improved fraud figures for the financial services industry. But that has to be seen in perspective: more than two-thirds (67%) of financial services companies were still hit by at least one fraud. Moreover, compared to other industries, the industry has some important problems. The sector had the highest level of internal financial fraud (25%) and regulatory or compliance breach (16%) of any industry, and the second largest rate of IP theft (10%). Information theft, however, remains the biggest problem. It affected 30% of financial services firms last year—the second highest prevalence of any sector. Moreover, companies in this sector were also the most likely to report that outside hackers were involved in the attacks on information (32%). Insiders, though, are also a problem—the same number of companies reported that employee malfeasance had been a factor in the attack. With increasing IT complexity cited as the leading driver of increased exposure to fraud (31%), it would make sense for financial services companies to boost their defences in this area. In light of the extent of these computer-based vulnerabilities, it is surprising that only 54% of financial services firms plan to invest in further IT security, barely above the overall survey average of 53%.

**Loss:** Average percentage of revenue lost to fraud: 0.7%

**Prevalence:** Companies affected by fraud: 67%

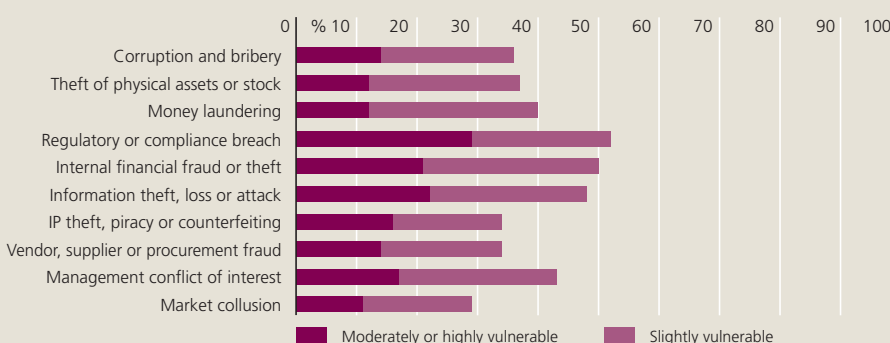
**Areas of Frequent Loss:** Percentage of firms reporting loss to this type of fraud:

Information theft, loss or attack (30%) • Internal financial fraud or theft (25%)

Regulatory or compliance breach (16%)

**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: IT complexity (31%)





# Organized crime penetration in Italian and European businesses

By Marianna Vintiadis

This year's Global Fraud Survey shows encouraging signs that European companies are becoming more alert to the requirements of anti-corruption legislation such as the US FCPA and the UK Bribery Act. Businesses have begun to adapt their policies and processes, but so too have fraudsters and other criminals. Over the last year, we have seen several cases which indicate that organized crime penetration is becoming increasingly prevalent within apparently sound business environments and that it is spreading into new territories. How has this happened?

In 2009, the head of the UN Office on Drugs and Crime, Antonio Maria Costa, suggested that in the aftermath of the 2008 banking crisis, the proceeds of organized crime were used to save a number of banks. Based on information received by intelligence agencies and prosecutors, Costa estimated that a majority of the \$352 billion in drug trafficking profits earned since 2008 had entered the global economic system. Now, several Italian and international agencies which evaluate organized crime activities and their proceeds are becoming increasingly concerned with the extent to which these funds are entering “normal” business sectors. This year’s anti-mafia report<sup>1</sup> by Confesercenti – the association of Italian small and medium enterprises – estimates that Italian organized crime has €65 billion in cash reserves and that profits last year reached €100 billion, approximately 7% of Italian GDP. This makes the Mafia Italy’s most liquid, and potentially its largest, “bank.”

One of Confesercenti’s most important concerns is usury, as small companies, strapped for cash and unable to obtain funds from the banking system, turn to loan sharks to meet their needs. There is, though, increasing evidence from recent prosecutions and reports that organized crime is utilizing the financial system in more sophisticated ways. Various intermediaries representing front companies, often registered in foreign countries, will offer businesses financing at market rates, sometimes in exchange for an ownership share in the company.

In today’s global economy, the problem has spread well beyond the Italian border. In June 2012, during a hearing of the European Commission’s Special Committee on Organized Crime, Corruption, and Money Laundering, the Italian anti-mafia prosecutor, Pietro Grasso, declared that Italian authorities tend not to pursue organized crime assets that lie outside of Italy. As a result, much of that crime-tainted capital now resides in other jurisdictions.

The expansion of organized crime into Germany has been particularly significant due to the great migratory wave to that country in the late 1950s from the province of Calabria. The ‘ndrangheta – the Calabrian mafia – is currently thought to control around 80% of drug trafficking in Europe, earning €27 billion a year from this crime alone, according to Italian daily La Repubblica. The newspaper adds that the organization, engaging in a mix of legal and illegal activities “has colonized the whole of the EU. US government experts rank this criminal

multinational fourth in the list of the world’s most dangerous organizations, after Al Qaeda, the PKK and the Mexican narco-traffickers. And Germany is its second home.”<sup>2</sup>

Germany is not the only country affected. Due to the integral part they play in the drug trade, major ports across Europe are also tainted by the organization’s presence: Antwerp, Barcelona, Piraeus, and Rotterdam are all beginning to appear in police and intelligence reports as having been infiltrated by the ‘Ndrangheta.

Across the Atlantic, the United States government has recently taken action against another Italian group, the Neapolitan *Camorra*. Last year, President Obama identified it as a transnational criminal organization. In August of this year, the Treasury Department identified Antonio Iovine, Michele Zagaria, Mario Caterino, Paolo Di Mauro, and Giuseppe Dell’Aquila as leaders or senior members of the *Camorra*. United States citizens are now prohibited from conducting financial or commercial transactions with these men and the Treasury has the authority to freeze any of their assets that are held in a US jurisdiction.

The new, sophisticated *mafioso* is a far cry from the stereotypical gangster image. Investments in stocks, real estate, and other investment vehicles typically require family members without prior convictions, who have sophisticated financial knowledge as well as the ability to complete complex transactions, often involving offshore entities.

Companies seeking to comply with current anti-money laundering and anti-corruption legislation must be aware of the risk of organized crime penetration into their business. Larger companies can normally rely on major financial institutions for financing, but this may not be an option for small and medium enterprises, who might look to other sources. Furthermore, where a company’s compliance protocols require suppliers to subscribe to their ethics code, a more rigorous third party screening process may be required.

Another potential problem for businesses is the perception that certain sectors are unlikely to be targeted by organized crime. In the past, the sourcing of third parties in sectors such as waste collection and recycling, gaming, and construction would immediately trigger a higher level of scrutiny during the due diligence process. Today, all sectors must be aware of the potential risks and conduct the appropriate level of reputational, operational, and commercial

due diligence. One example is the restaurant trade. Evidence of flourishing illegal activity in this sector can be found in Germany, where the German Federal Criminal Police Office has suggested that the Romeo-Pelle-Vottari clan alone runs 55 restaurants in the eastern German states of Saxony and Thuringia, as well as in the Ruhr region.<sup>3</sup>

The alarming penetration by organized crime of the renewables industry has also hit headlines in recent years: 126 arrests were made between 2007 and 2011 in relation to Italian wind farms alone. The latest reports issued by the Italian anti-mafia task force reveal that Sicilian and Calabrian clans have managed to occupy entire chains of production, transportation, and sale of agricultural and fishing products, reaching an annual turnover of €9.5 billion.

As a result of the economic crisis and the attendant financing needs of companies and entrepreneurs, organized crime has been given the opportunity to find new ways to penetrate a variety of sectors. Additionally, the huge cash holdings derived from illegal activities such as racketeering and drug trafficking, have opened the door to new ways to launder ill-gotten gains. At the same time, as global markets continue to evolve, so too does the mafia’s *modus operandi*. As a result, assets are now frequently stored abroad and concealed by fiduciary off-shore entities, often managed and represented by “clean” and skilled professionals who cannot be identified as affiliates.

The current infiltration of organized crime into a variety of business sectors and geographical areas confirms its ability to diversify and adapt. Companies must therefore ensure that their due diligence and compliance programs are sufficiently robust in order to protect their business and their reputation from this growing threat.



**Marianna Vintiadis** is Kroll’s Country Manager for Italy and Greece, and also works with clients in Austria and Switzerland. 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, internal investigations, litigation support and internet investigations.

1 Le mani della criminalità sulle imprese – XIII Rapporto di SOs Impresa

2 “Duisburg, province of Reggio Calabria – The ‘Ndrangheta find a second home”, June 22, 2012

3 “Inside the World of the ‘Ndrangheta,” Der Spiegel, April 1, 2012

# RUSSIA OVERVIEW



Although the overall prevalence of fraud in Russia (61%) is identical to the survey average, a number of individual frauds are markedly more common than in the rest of the world. These include information theft (26% compared to 21% globally), corruption and bribery (16% compared to 11%), and IP theft (13% compared to 8%).

	2011-2012*
<b>Prevalence:</b> Companies affected by fraud	61%
<b>Areas of Frequent Loss:</b> Percentage of firms reporting loss to this type of fraud	Theft of physical assets or stock (26%) Information theft, loss or attack (26%) Corruption and bribery (16%)
<b>Areas of Vulnerability:</b> Percentage of firms considering themselves moderately or highly vulnerable	Internal financial fraud (26%) Information theft, loss or attack (16%) Corruption and bribery (16%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	52%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	Entry into new, riskier markets (23%)
<b>Loss:</b> Average percentage of revenue lost to fraud	0.4%

\*Insufficient respondents in 2011 to provide comparative data.

Russian respondents, however, do not seem to appreciate the risk. For all three of the above frauds, the proportion who consider their companies moderately or highly vulnerable is markedly below the global average. For information theft in particular, only 16% describe their companies in this way, which is just over half of the overall survey figure (30%) and much lower even than the number of companies reporting that such a fraud occurred during the last year (26%). Meanwhile, although entry into new, riskier markets, was the leading cause of increased fraud exposure this year (23%), Russia was the only country or region where none of the respondents reported that their companies were dissuaded from doing business anywhere in the world out of concern about corruption risks.

In terms of fraud perpetrators, collaborators with the company are a serious threat. Of businesses affected by fraud in the last year and where the perpetrator was known, 42% report that an agent or intermediary was a leading participant – the highest figure for any country – and 21% say the same about partners – the second highest figure after Colombia. Russian companies, however, are slightly less likely than average to plan to invest in improved partner due diligence in the next 12 months (35%).



## Russia's undisclosed silent partners: Knowing who you're dealing with

By Alessandro Volcic and William Scott-Gall

**The results of the 2012 Global Fraud Survey support the widely-held view that Russian businesses suffer disproportionately from exposure to corruption. Companies in Russia are approximately 50% more likely than the global average to have experienced an incident of bribery or corruption during the last year.**

The perception of corruption in Russia is also particularly high, as illustrated by Transparency International's Corruption Perceptions Index – Russia ranks 143rd (on a par with Nigeria and Uganda). The Russian government has, however, recently taken a significant step toward improving the country's reputation by adopting international anti-bribery standards: in April 2012, Russia became the 39th party to the OECD Anti-Bribery Convention. This is undoubtedly good news for those looking to invest in Russia, but careful due diligence is still critical to success.

Changes in the global regulatory environment, such as the implementation of the UK Bribery Act 2010, have encouraged investors and counterparties to carry out deeper due diligence, especially in high-risk markets. In Russia, the due diligence process is greatly impeded by the prevalence of undisclosed

silent partners as investors or shareholders in companies. This can be a major source of risk, as their involvement is undocumented: business owners often prefer to use oral agreements, making identification of these individuals during the due diligence process more difficult. In some cases, such an agreement can give a silent partner either a stake in a business or a share of the proceeds of a particular transaction. The existence of the interest is often well known in the market but, as it has never been documented, the specific terms may be unclear. These arrangements may be used to make corrupt payments to government officials, or enable them to disguise their economic interest in a project.

This sort of informal, undocumented relationship has grown somewhat less frequent since the 1990s, but it remains

common and is underpinned by two important factors: first, deals are often struck with close, trusted contacts who already have a long history together and strong personal relationships; second, businesses are reluctant to put sensitive information about their activities in writing, lest it be exploited by law enforcement, taxation agencies, or corporate raiders.

One way that silent partners feature in Russian business life is when *krysha* comes into play. *Krysha*, the Russian word for “roof”, is the slang term that refers to providing protection or political support. The role of *krysha* and silent partners has been subjected to unprecedented legal scrutiny in London's Commercial Court this year. In August, the court ruled that an oral agreement between Boris Berezovsky and Roman Abramovich, two noted Russian investors, was akin to a *krysha*-style obligation.

In September, Oleg Deripaska, another Russian businessman and majority owner of the world's largest aluminium producer, Rusal, settled a dispute out of court with his former partner, Mikhail Chernoy. These cases and others besides have attracted significant media attention and shed light not only on the high-risk deal making of the 1990s, but on how business is done in Russia today.

London's rise as the global centre for dispute resolution and a preference among investors and advisers to conduct transactions under English law both serve to protect investors, to some extent, from the worst problems associated with doing business in Russia. Ultimately, though, it is essential to know who your potential partners really are, by conducting rigorous due diligence.



**Alessandro Volcic** is a Senior Director in Kroll's Moscow office. Alex has been involved in and led complex international fraud investigations, internal investigations, multi-jurisdictional asset recoveries and business intelligence assignments.

Alex specializes in Russia, the former Soviet Union and Central Europe, but has also conducted cases in Germany and the Middle East.



**William Scott-Gall** is an Associate Director in Kroll's London office. William has worked on a variety of projects in areas such as litigation support, asset recovery, reputation management and due diligence investigations. He primarily works on cases involving emerging markets in Central and Eastern Europe/FSU countries and in the natural resources sector.

# THE GULF STATES OVERVIEW



Respondents from the Gulf States, including Saudi Arabia, report a lower prevalence of fraud than the global average (61%), with just fewer than half of companies being affected by at least one such crime in the last year. The prevalence levels of three particular frauds, though, are within one percent of the global average: management conflict of interest (15%), corruption (10%), and regulatory breach (10%).

Moreover, these are often linked, with most cases of corruption also involving management conflict of interest. Whether this results from major steps taken by countries such as Saudi Arabia to address corruption or a potentially dangerous underestimate of what lies beneath the surface is unclear.

The main perpetrators of fraud in the Gulf differ in some ways from the norm. Insiders are as likely in the region as elsewhere to be involved: 68% of companies that reported a fraud and knew the culprit said it was either an employee or an agent and in 85% of cases of information theft employee malfeasance was to blame. More striking, however, 26% of frauds involved a government official or regulator in the Gulf, compared to just 14% worldwide. This does not mean that the region's officials are inherently less trustworthy than in other regions: the survey puts corruption levels in the Gulf slightly below the global average. Instead, the relative absence of other types of fraud throws into sharper relief one of the problems that does exist – a tendency of some managers and officials to work together in inappropriate ways.

This issue should be addressed. Although companies in the region are more active than most in fraud prevention – they are much more likely than average to be planning to invest in every anti-fraud strategy covered by the survey – they are not addressing the risk of corruption nearly as aggressively as their peers. For Gulf companies affected by the US FCPA and the UK Bribery Act, for example, over half have not trained senior staff, vendors and foreign employees in complying with these laws, compared to just 28% worldwide.

	2011-2012
<b>Prevalence:</b> Companies affected by fraud	49%
<b>Areas of Frequent Loss:</b> Percentage of firms reporting loss to this type of fraud	Theft of physical assets or stock (18%) Management conflict of interest (15%)
<b>Areas of Vulnerability:</b> Percentage of firms considering themselves moderately or highly vulnerable	Information theft, loss or attack (28%) Management conflict of interest (24%) Regulatory or compliance breach (24%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	54%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	Entry into new, riskier markets (23%)
<b>Loss:</b> Average percentage of revenue lost to fraud	0.5%

\*Insufficient respondents in 2011 to provide comparative data.



# Kingdom of Saudi Arabia: Time to bridge the perception gap

By Yaser Dajani

**Saudi Arabia is the largest economy in the Middle East, and is growing ever more powerful: the country's GDP grew by almost 7% last year to \$618 billion. Despite the ability of neighbouring Doha, Abu Dhabi and Dubai to grab headlines, it is worth remembering that Saudi Arabia's economy is almost 60% larger than the United Arab Emirates and more than three times the size of Qatar. The Saudi government remains committed to sustaining fast-tracked growth. Demographics alone is a compelling reason: with a population of 29 million people, unemployment is a looming problem, made all the more pressing by the Arab Spring sweeping through the Middle East and North Africa.**

The Ministries of Housing, Interior, Defense, Health, Telecommunications, Industry, Oil, and Social Affairs are currently driving ambitious spending programs for infrastructure development across all sectors of the economy. Despite the global economic downturn in 2009 from which many countries in the Gulf have yet to recover, Saudi Arabia's infrastructure expenditure – with \$184 billion budgeted this year – continues to provide meaningful momentum, and a host of opportunities for domestic, regional and international private sector players. In 2013 the country will witness the completion of many ambitious construction programs, and although there are natural

dips in the award of contracts, these are attributed to delays in government procedures, not the country's motive or intent.

This acceleration of growth and opportunity carries concomitant problems. With more companies from other parts of the Gulf, Asia, Europe, and the United States – the Kingdom's largest trading partner – entering the Saudi market and forming joint ventures with local businesses, there comes an increased potential for fraud and corruption. The ingredients are there on the table: cross-border joint ventures with new counterparties; limited transparency; government-led development programs and a broad interface between the public and

private sectors; technologically complex, large-scale, and intertwined projects with unwieldy international consortia; and an unfamiliar legal environment to navigate.

In recent years, Saudi Arabia has introduced robust measures to enhance its drive to fight corruption. The first move was the issuance of the National Strategy for Maintaining Integrity and Combating Corruption adopted in 2007, which provided the blueprint for fighting corruption. Perhaps the boldest move was the decision by the King to establish the National Anti-Corruption Commission in 2011. This commission has direct oversight of all government bodies and corporate entities in which the government holds a 25% or

greater equity stake. The commission is tasked with raising awareness of corruption, investigating and combating it, and ensuring the return of embezzled funds. The body's creation was prompted, at least in part, by a number of recent high-profile debacles in the Kingdom, including the Al Gosaibi-Maan Al Senea dispute and the Jeddah flooding. The government's investigation into the latter recently led to a Saudi public official and businessman being jailed for five years and fined for receiving and paying bribes.

A number of other bodies are also responsible for fighting corruption in the country, including the Prosecution and Investigation Commission, the General Auditing Bureau, and the Auditing and Investigation Commission. The legal basis for these initiatives is embodied in a series of decrees and laws passed by the King and ratified by the Council of Ministers. Although Saudi laws generally deal with the behavior of public officials rather than private commercial bribery, the government has made good progress towards regulating the public sector and laying the platform for a stringent compliance environment.

Some Saudi businesses, however, are lagging behind and have yet to develop mature internal compliance mechanisms and procedures. This is more than a question of insufficient compliance processes of domestic operations: the rapidly accelerating globalization of Saudi enterprise (e.g. non-hydrocarbon exports increasing 34% on last year to \$42 billion), may be an economic success story, but it can also be a multiplier of risks.

In this year's Global Fraud Survey, 56% of respondents in Saudi Arabia said that their companies did not suffer from any type of fraud in the past year. Moreover, for every fraud covered in the survey, about 80% of respondents or more believed that they were at most only slightly vulnerable. From what Kroll has seen, there is clearly a wide gap between the perception of threat and the actual risk that Saudi businesses are facing in both domestic and foreign markets.

This severe underestimation of the prevalence of fraud is particularly worrying: there is no more effective way to invite attack than to lower defenses. In our experience, the wider this gap grows, the greater the real risk becomes, and the greater the need for anti-corruption programs and training. Regrettably, it is also our experience that

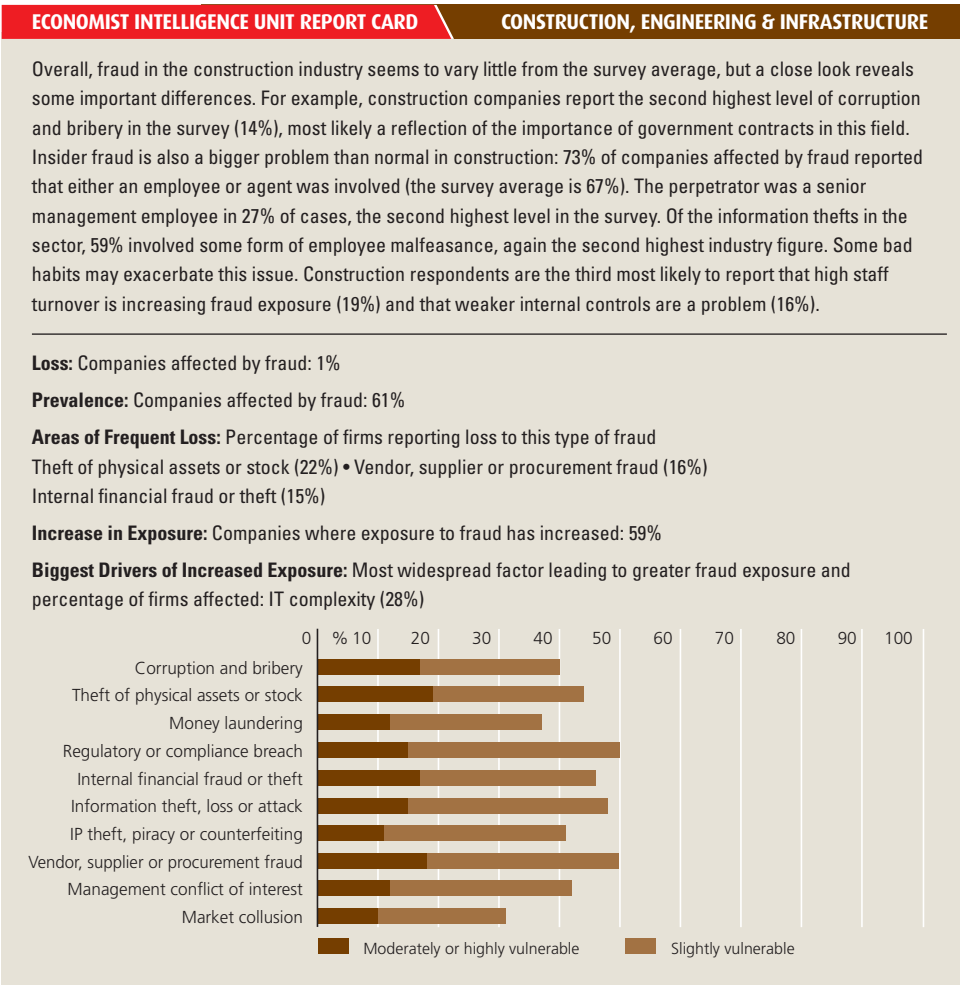
those who have been impacted by fraud are the fastest learners, and those that have not are more inclined to sweep the problem under the carpet until they have. Put simply, there are specific risks faced by foreign investors in Saudi Arabia, local businesses partnering with foreign entities on domestic contracts, and by Saudi Arabian entities exporting products, services, and capital to uncharted territory.

Companies need to develop a deep understanding of counterparties, and to conduct a risk assessment of the transactions and the key principals surrounding them. Although fraud comes from multiple directions and sources, the main ones we have seen in Saudi Arabia involve management conflict of interest, theft of physical assets, regulatory breaches, and bribery. The good news is that 62% of Saudi businesses participating in the survey now have some form of pre-transaction due diligence in place. More interesting is that 88% of respondents indicated that they have a well-defined whistleblower process, which perhaps reflects that Saudi businesses are now beefing up their corporate governance structures.

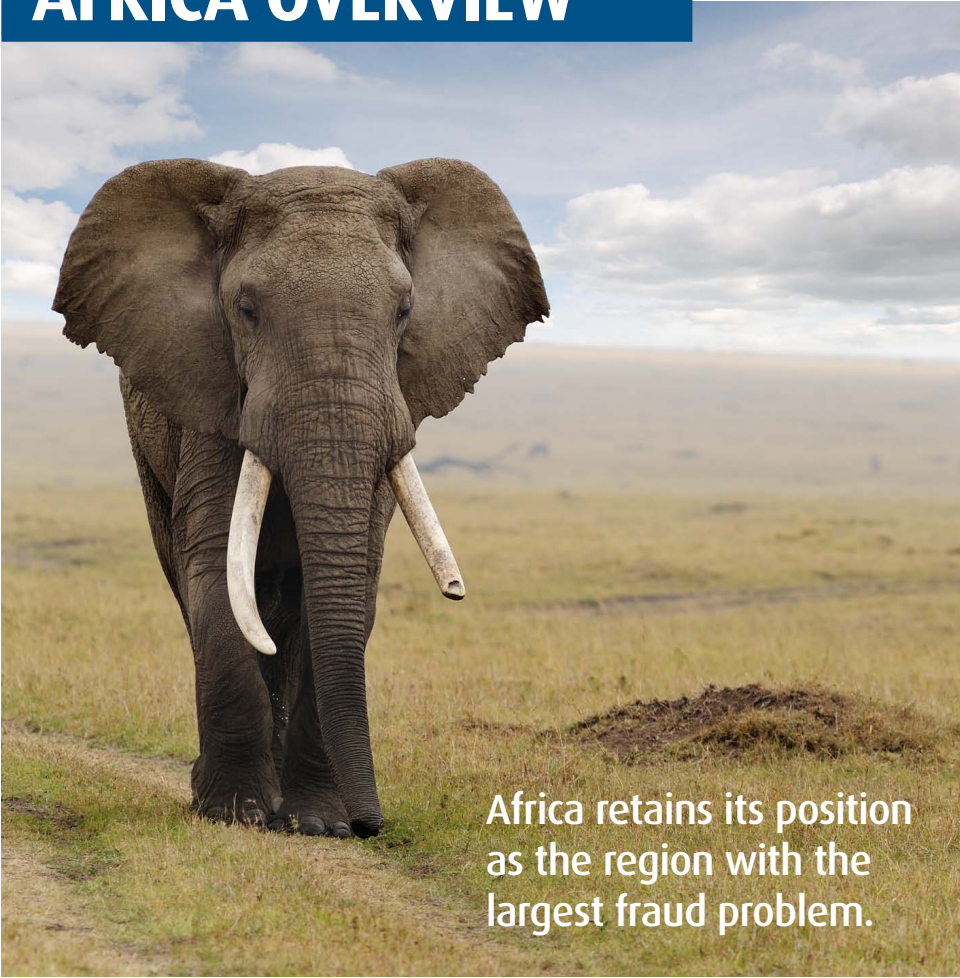
Based on these figures and our experience in the market, it would appear that systematic methods toward risk management and mitigation have been adopted by some of the leading Saudi corporations and private offices. Our experience also shows that more and more companies in the Kingdom are now engaging external specialists and risk consultants to conduct fraud-related investigations as well as to design and implement fraud prevention programs. However, they remain in the minority and many still make the mistake of assuming that lawyers and accountants alone can provide sufficient protection. This itself would suggest there is some pain to come, and the consequences could prove far-reaching and have considerable financial repercussions.



**Yaser Dajani** is an Associate Managing Director in Kroll's Middle East practice. Yaser manages investigations for regional and international businesses and government clients. His core areas of expertise include complex business intelligence, market entry support, corruption risk assessments, reputational management, asset searches, litigation support and dispute advisory. He works across a wide range of sectors and geographies in the Middle East and North Africa.



# AFRICA OVERVIEW



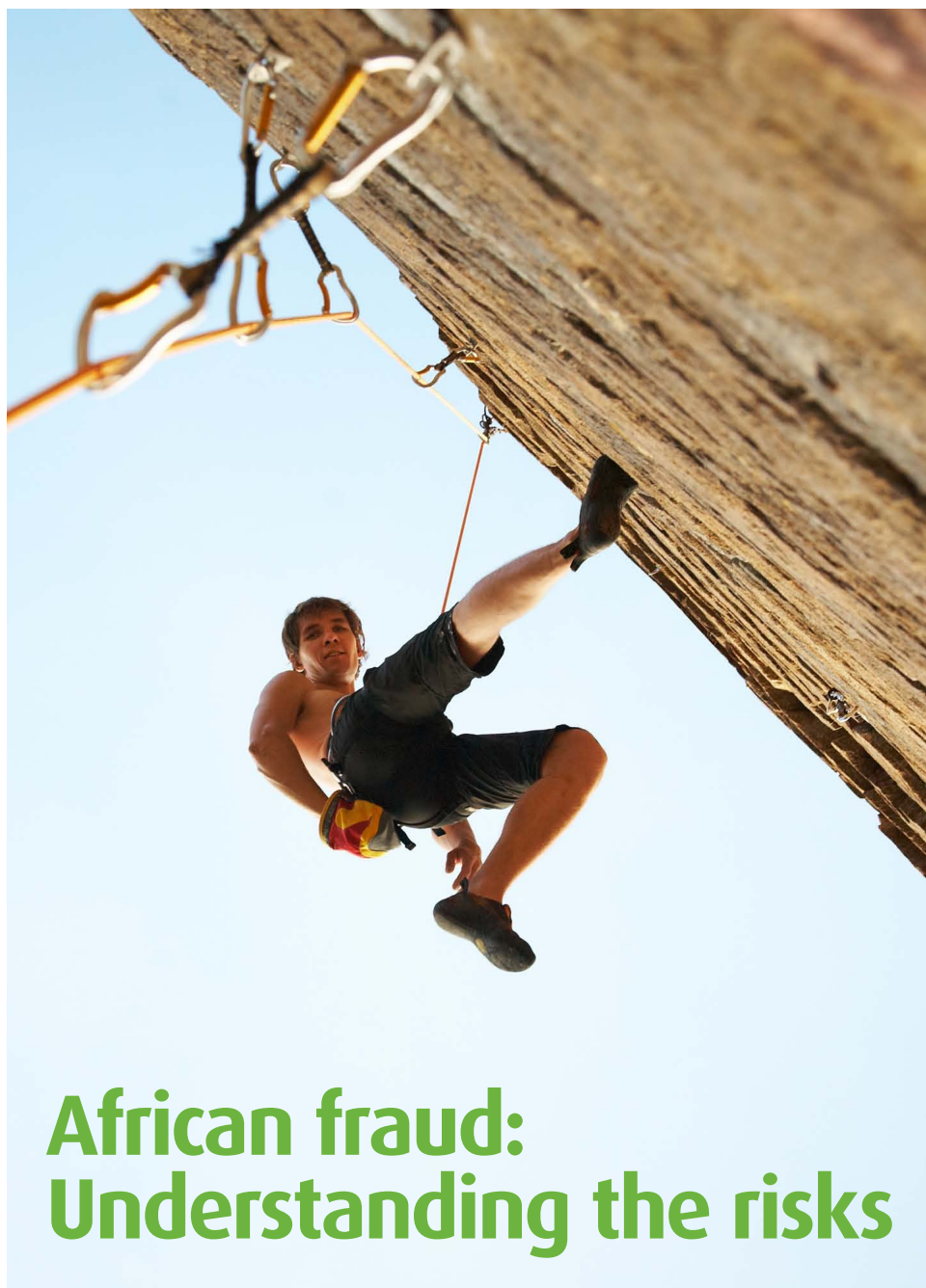
Africa retains its position as the region with the largest fraud problem.

It did see some improvement in the fraud environment, but the decline in overall fraud prevalence, from 85% to 77%, was less marked than in other regions. As a result, it has not only the greatest overall fraud figure, but also the highest regional prevalence for eight of the 10 frauds covered in this index: information theft (34%); theft of physical assets (32%); internal financial fraud (30%); management conflict of interest (25%); corruption and bribery (20%); intellectual property theft (11%); market collusion (11%); and money laundering (2%). It also has the highest regional levels of perceived vulnerability to these same eight crimes.

The specific fraud challenges in Africa shifted somewhat in the last year. Information theft became a predominant problem, affecting 34% of all companies, up from 22% the year before. Currently 42% of African respondents believe that their companies are moderately or highly vulnerable to such attacks, but this may rise in future as 50% say that increasing IT complexity is the primary driver of increased fraud exposure at their firms. The information being sought is also markedly different in Africa compared to elsewhere: in 53% of cases where an information attack took place and the target was known, fraudsters were looking for internal company strategic plans and data, well above the survey average of 29%. What such theft has in common with much of the world, however, is the large number of insiders involved: employee malfeasance played the leading role in 37% of such cases. This should come as no surprise, given that 82% of all frauds on the continent involved either an employee or agent of the company as important participants.

On the positive side, the number of companies reporting an incident of corruption in the past year (20%) dropped, although this is still the highest regional figure. One reason for the continued problems in this area seems to have been a relative lack of attention to it. Africa is the only region where fewer than half of companies for which it is relevant have made a thorough assessment of risks arising from the US FCPA or the UK Bribery Act, or which have included such considerations in their due diligence activities. The costs for the continent's slow progress in fighting corruption continue to mount up. This year 9% of all companies were dissuaded from doing business there, and 61% of these said that corruption was a major consideration when they decided not to enter a region.

	2011-2012	2010-2011
<b>Prevalence:</b> Companies affected by fraud	77%	85%
<b>Areas of Frequent Loss:</b> Percentage of firms reporting loss to this type of fraud	Information theft, loss or attack (34%) Theft of physical assets or stock (32%) Internal financial fraud or theft (30%) Management conflict of interest (25%) Corruption and bribery (20%)	Theft of physical assets or stock (38%) Corruption and bribery (37%) Internal financial fraud or theft (33%) Vendor, supplier or procurement fraud (31%) Management conflict of interest (27%) Information theft, loss or attack (22%)
<b>Areas of Vulnerability:</b> Percentage of firms considering themselves moderately or highly vulnerable	Internal financial fraud (49%) Corruption and bribery (45%) Information theft, loss or attack (42%)	Corruption and bribery (78%) Theft of physical assets or stock (68%) Internal financial fraud (67%)
<b>Increase in Exposure:</b> Companies where exposure to fraud has increased	73%	84%
<b>Biggest Drivers of Increased Exposure:</b> Most widespread factor leading to greater fraud exposure and percentage of firms affected	IT complexity (50%)	Weaker internal controls (35%)
<b>Loss:</b> Average percentage of revenue lost to fraud	1.6%	3.1%



## African fraud: Understanding the risks

By Alexander Booth and Melvin Glapion

**In 2012, as the vogue for Africa as an exciting new investment frontier perhaps approaches its apogee, the continent nevertheless remains affected by the prevalence, and to an even higher degree the perception of fraud and corruption, which often dissuades international companies from investing and operating in the region.**

In this year's Global Fraud Survey, over 40% of respondents identified their operations in Africa as moderately or highly vulnerable to the threats of internal financial fraud, corruption and bribery and information theft. The numbers probably say more about what business people are thinking than about the true scale of the problem, but the message is clear: fraud in Africa is a pervasive issue.

The data from the survey also points to two interesting trends. First, the threat is moving away from the physical and towards the technological. In the past 12 months, 32% of

companies experienced a theft of assets or physical stock (fewer than last year), while 34% suffered from information theft (a significant increase on last year), and 11% fell victim to intellectual property theft or counterfeiting (also up). Much of the information loss occurred through the theft of devices, such as hard-drives, or the compromising of IT systems. In Africa, sophisticated external penetration is rare: people with inside access are usually to blame.

Second, the perpetrators of fraud tend to operate from the lower ranks of the company; the survey found that junior employees are key players in 56% of frauds suffered by African companies, whereas 24% of senior employees and managers are involved. While it's less common for senior managers to be linked to certain types of fraud – for example the misappropriation of assets, they can be implicated in other ways. This is highlighted by some 40% of the African companies surveyed who say that they are moderately or highly vulnerable to management conflict of interest.

The conclusions that can be drawn from these statistics are not merely academic. Fraud continues to have a tangible negative impact on the commercial performance of businesses operating in Africa: the Global Fraud Survey shows that over 11% of these companies estimated their fraud-related losses to be more than 4% of their total revenues. This is nearly twice as high as the survey average. Moreover, fraud is deterring foreign investment: 9% of companies worldwide were dissuaded from doing business in Africa in the last year because of perceived fraud levels – a far higher figure than for any other region.

Looking beyond the numbers, the financial and reputational consequences for companies implicated in fraud in Africa can be severe. A number of recent, prominent cases provide a salutary reminder to the international business community of the dangers of getting it wrong.

In July this year, the World Bank banned two African subsidiaries of the prestigious Oxford University Press (OUP) from doing business with it for three years over fraudulent practices. The companies – Oxford University Press East Africa Limited in Kenya and Oxford University Press Tanzania Limited – were found to have made improper payments to government officials for two contracts to supply text books in relation to World Bank-

financed projects. OUP agreed to pay a fine of \$500,000 as part of a negotiated resolution. In 2010, the World Bank had imposed a similar six-year ban on business with Macmillan Publishers Limited because of fraud and bribery concerns linked to an education project in Sudan.

More recently, in September 2012, the former head of French oil giant Elf, Loik Le Floch-Prigent, appeared in court in Togo charged with being an accessory to fraud. The case involves a complaint from an Emirati businessman who alleges that he was the victim of a \$48 million embezzlement scheme facilitated by Le Floch-Prigent while at Elf. Togo's former Minister of Territorial Administration, Pascal Bodjona, has also been charged in the case, as well as Togolese businessman Bertin Sow Agba.

Institutional and governmental efforts by African countries to combat fraud are being launched with increasing frequency, but with varying levels of dedication and resource provision, and with correspondingly mixed results. The most progress to date appears to have been made by South Africa, where there is an increasing determination to stamp out fraud and corruption. Several recent cases show that even top officials are not immune to prosecution and disgrace following prosecution under anti-corruption legislation including the FCPA and UK Bribery Act 2010.

Earlier this year, General Bheki Cele, the National Police Commissioner, was suspended and a board of inquiry established to investigate his allegedly fraudulent manipulation of a tender process for new police headquarters in Pretoria and Durban. Similarly, Nehawu, one of South Africa's largest and most influential public sector unions, has called for Humphrey Mmemzi, until recently Local Government and Housing Minister of Gauteng – the province which includes Johannesburg and Pretoria – to be investigated over a fraud involving corporate funds. Both of these cases have been closely covered by the South African media, underscoring the importance of a free press to continuously monitor and report fraud and hold its perpetrators accountable. Other African countries, though, lag behind in the sophistication of their media and the transparency of their business environment.

In some states, weak governance has combined with local demographic factors to produce a fraud threat to which Africa is acutely vulnerable: counterfeit

pharmaceuticals. Across the continent, counterfeiting networks exploit poor national drug regulation systems to sell medicines with little or no active ingredient. The scale of the HIV epidemic across Africa makes the trade in counterfeit anti-retroviral drugs particularly lucrative: one of the largest corporate frauds ever recorded in South Africa took place in 2009 when Australia-based businessman Barry Tannenbaum reassured funders by forging hundreds of orders for AIDS drugs. Of course, such activity is not only highly damaging to the brand, reputation, and profitability of legitimate pharmaceutical manufacturers – such as Sanofi-Aventis, GlaxoSmithKline, and Merck – but can have all too tragic implications for patients. According to the World Health Organization, some 200,000 deaths could be prevented each year if the African trade in counterfeit drugs were reduced.

Africa remains a promising investment destination in many ways, but those who are thinking of investing in the region need to understand the risks. More than ever, companies and investors who succeed in

Africa will likely be those who have invested heavily in understanding the local political environment, background screening of third parties, training staff, and carefully implementing internal risk management systems.



**Melvin Glapion** is a Managing Director in Kroll's London office. He has over 16 years of M&A, corporate strategy and financial analysis experience, leading multidisciplinary and multi-jurisdictional teams in conducting cross-border market entry, due diligence and competitive intelligence engagements. He has worked on a broad range of engagements in Sub-Saharan Africa, including projects in Zimbabwe, Senegal, DRC and Nigeria.



**Alexander Booth** is a Senior Director with Kroll's London office, specializing in complex business intelligence assignments and emerging markets. He has also worked in Kroll's Dubai office, covering the Middle East and North Africa region. Recently, Alexander has been involved in a diverse range of cases, and developed particular expertise in managing networks of subcontractors and human sources in sensitive environments, particularly in DRC, Nigeria, Ghana and Angola.

#### ECONOMIST INTELLIGENCE UNIT REPORT CARD

#### HEALTHCARE, PHARMACEUTICALS & BIOTECHNOLOGY

The proportion of healthcare, biotechnology and pharmaceutical companies affected by at least one incidence of fraud (52%) was among the lowest of any industry and the percentage reporting an increase in fraud exposure (also 52%) was the second lowest. Every type of fraud covered in the survey also declined in prevalence. However, the sector needs to make improvements in the field of partnerships. Increasingly, life science sector companies—whether in health delivery or drug development—work with other organisations. Only 9% of respondents see increased collaboration as a factor that increases fraud exposure, but 13% of companies affected by fraud report that a partner was involved—the highest figure for any industry. At the moment, healthcare and biopharmaceutical companies are only slightly more likely than average to have partner, client and vendor due diligence in place, and in the next 12 months 43% plan to invest in it compared with 38% for the survey overall. This might be an area where further work will be worthwhile.

**Loss:** Average percentage of revenue lost to fraud: 0.9%

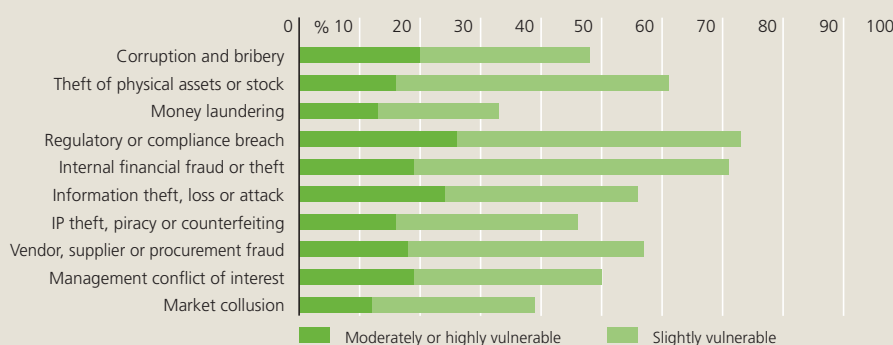
**Prevalence:** Companies affected by fraud: 52%

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

Theft of physical assets or stock (18%) • Information theft, loss or attack (18%)  
Management conflict of interest (16%)

**Increase in Exposure:** Companies where exposure to fraud has increased: 52%

**Biggest Drivers of Increased Exposure:** Most widespread factor leading to greater fraud exposure and percentage of firms affected: IT complexity (19%)



# Calm waters?

## Be aware of increasing fraud exposure



For the third year in a row, the travel, leisure and transportation industry saw the smallest proportion of companies in any sector hit by at least one incidence of fraud: just 50%.

### ECONOMIST INTELLIGENCE UNIT REPORT CARD

### TRAVEL, LEISURE & TRANSPORTATION

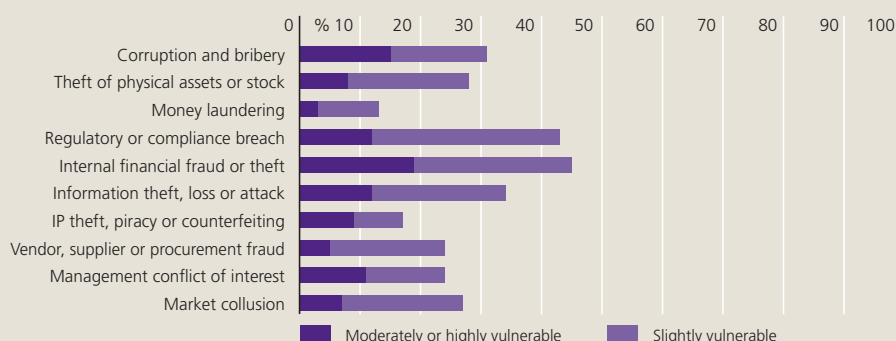
**Loss:** Average percentage of revenue lost to fraud: 0.6%

**Prevalence:** Companies affected by fraud: 50%

**Areas of Frequent Loss:** Percentage of firms reporting loss to this type of fraud  
Internal financial fraud or theft (22%) • Regulatory or compliance breach (16%)

**Increase in Exposure:** Companies where exposure to fraud has increased: 52%

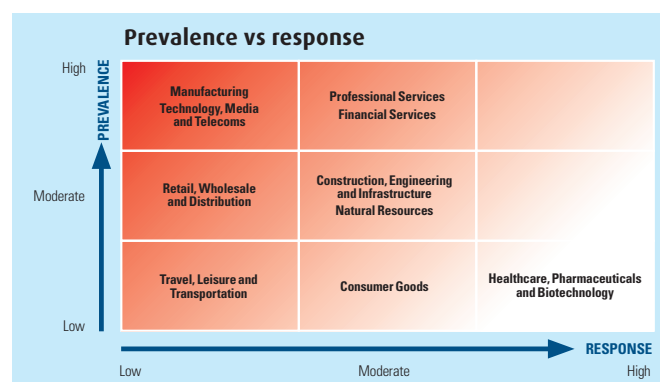
**Biggest Drivers of Increased Exposure:** Most widespread factor leading to greater fraud exposure and percentage of firms affected: IT complexity (36%)



Companies should be aware of two developments which could lead to bigger problems if left unaddressed. The first involves information theft. Although the prevalence of this problem at travel and leisure companies (14%) is well below the overall average (21%), it did rise from last year. IT complexity also remains the leading driver of increased fraud exposure (36%). More worryingly, over half the information attacks that took place in the past year targeted internal strategic plans or data (55%), the highest figure for any industry.

Another issue is the type of people involved in fraud at these companies. Where there has been a fraud and the perpetrator is known, travel and leisure companies are the most likely to report that an insider has been involved (88% of the time) and that senior management employees are involved (34%, or nearly twice the survey average of 18%). This is consistent with a marked rise in internal financial fraud in the sector, from 16% last year to 22% this year. It may also help explain why, even though the industry has the lowest overall incidence of fraud, it has only the third lowest average loss. Research in previous years has shown that fraud by senior management tends to be more expensive.

# Summary of sector fraud profiles



Sector	Prevalence (degree to which sector is exposed to fraud)	Response (degree to which sector has adopted or plans to further invest in fraud countermeasures)	Comment
Natural Resources	Moderate	Moderate	Despite a noticeable drop in the prevalence of fraud, Natural Resources companies continue to struggle with theft of physical assets, management conflict of interest and regulatory breaches. Moreover, more companies in the sector were hit by information theft this year, and, most often, proprietary financial data was targeted. Despite this growing threat, natural resources companies are somewhat less likely than the survey average to invest in greater IT protection.
Financial Services	High	Moderate	While the Financial Services sector experienced a drop in the overall prevalence of fraud, companies reported the highest incidence of internal financial fraud and regulatory compliance breach. Perhaps more worrisome, the sector logged the second highest level of information theft and more often than not, cited employee malfeasance as a factor in the attack. Even with the increasing insider threat, companies plan only moderate investment in strengthening IT security.
Manufacturing	High	Low	The Manufacturing sector reported the highest percentage of companies hit by fraud in the last year, with substantial increases in eight of the 10 frauds covered in the survey. These include the highest levels of theft of physical assets, corruption, management conflict of interest, vendor or procurement fraud, and IP theft. The sector also recorded the highest average loss to fraud. Despite these growing threats, manufacturing companies plan substantially below average investment for almost every anti-fraud strategy covered in the survey over the coming 12 months.
Construction, Engineering & Infrastructure	Moderate	Moderate	While the Construction, Engineering & Infrastructure industry saw a modest decline in the prevalence of fraud this year, the percentage remains high compared to other sectors, and more often than not, the fraud was committed by an insider. Companies cite high staff turnover as a leading cause for increased exposure, followed by lower investment in internal controls procedures.
Retail, Wholesale & Distribution	Moderate	Low	The Retail, Wholesale and Distribution sector experienced average levels of fraud, nearly two-thirds of companies report being hit at least once, and theft of physical assets remains a major issue for the sector. Retail, wholesale and distribution companies are most likely to report fraud involving customers and vendors, however investment in anti-fraud measures such as client and vendor due diligence is below the survey average.
Technology, Media and Telecoms	High	Low	Despite the high prevalence of fraud reported by companies in the Technology, Media and Telecommunications sector, companies in the sector are less likely than average to have in place any of the 11 anti-fraud strategies covered in the survey. Moreover, fewer TMT companies than the survey average plan to invest in nine of those measures. Information theft remains the biggest problem for companies in the sector.
Consumer Goods	Low	Moderate	The Consumer Goods sector posted the second lowest percentage of companies affected by fraud and saw drops in all but one of the frauds covered in the survey. However, vendor or procurement fraud and theft of physical assets continue to be major issues for the sector. Even so, adoption of anti-fraud strategies to combat these problem areas remains at average levels or below average, compared to other industries.
Healthcare, Pharmaceuticals and Biotechnology	Low	High	The Healthcare, Pharmaceuticals and Biotechnology industry reported the second lowest percentage of companies hit by fraud. Amid the good news are areas of concern. The sector posted the highest percentage of fraud involving external partners, and companies are only slightly more likely than the survey average to have partner, client and vendor due diligence programs in place.
Professional Services	High	Moderate	This year, the Professional Services sector reported the second highest percentage of companies affected by fraud. The industry saw increases in seven of the ten frauds covered in the survey, most notably a substantial rise in the number of companies reporting theft of physical assets and information theft. In fact, companies in the sector reported the highest levels of information theft of all industries. Respondents cite IT complexity as the leading cause for increased fraud exposure.
Travel, Leisure and Transportation	Low	Low	For the third year, the Travel, Leisure and Transportation sector reported the lowest levels of fraud, even as companies in the sector posted notable increases in internal financial fraud and information theft. It also cited the highest levels of insider fraud and involvement of senior management in those acts, when the perpetrator was known. Despite these increasing threats, investment in most anti-fraud strategies covered in the survey remains low.

# Key regional contacts at Kroll Advisory Solutions

For information about any of Kroll's services, please contact a representative in one of our offices below.

## Corporate

### Headquarters

600 Third Avenue  
New York, NY 10016

## Global

### Representatives

#### North America

David Holley  
Boston  
1 617 210 7466  
dholley@kroll.com

#### Latin America

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

#### United Kingdom

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

#### Europe, Middle East & Africa

Tom Everett-Heath  
London  
44 207 029 5067  
teverettheath@kroll.com

#### Asia

Tadashi Kageyama  
Hong Kong  
852 2884 7788  
tkageyama@kroll.com

## Local Offices

#### North America

Richard Plansky  
New York  
1 212 593 1000  
rplansky@kroll.com

Ray Blackwell  
Bastrop  
1 512 321 4421  
rblackwell@kroll.com

David Holley  
Boston  
1 617 210 7466  
dholley@kroll.com

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

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

Brian Lapidus  
Nashville  
1 866 419 2052  
blapidus@kroll.com

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

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

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

Peter McFarlane  
Toronto  
1 416 682 2784  
pmcfarlane@kroll.com

Michael DuBose  
Washington  
1 202 772 2039  
mdubose@kroll.com

#### Latin America

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

Recaredo Romero  
Bogota  
57 1 742 5556  
rromero@kroll.com

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

Ernesto Carrasco  
Mexico City  
52 55 5279 7250  
ecarrasco@kroll.com

Frederico Gebauer  
São Paulo  
55 11 3897 0900  
fgebauer@kroll.com

#### Asia

Colum Bancroft  
Hong Kong  
852 2884 7788  
cbancroft@kroll.com

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

Reshmi Khurana  
Mumbai  
91 22 6724 0500  
rkhurana@kroll.com

Violet Ho  
Shanghai  
86 21 6156 1700  
vho@kroll.com

Abigail Cheadle  
Singapore  
65 6645 4520  
acheadle@kroll.com

Makoto Suhara  
Tokyo  
81 3 3509 7100  
msuhara@kroll.com

#### Europe, Middle East & Africa

Brian Stapleton  
London  
44 207 029 5126  
bstapleton@kroll.com

Brendan Hawthorne  
Dubai  
971 4 449 6716  
bhawthorne@kroll.com

Arturo Melero  
Madrid  
34 91 274 7954  
amelero@kroll.com

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

Alessandro Volcic  
Moscow  
7 495 969 2898  
avolcic@kroll.com

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

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 Advisory Solutions 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 Advisory Solutions. Clients may distribute for their own internal purposes only. Kroll Advisory Solutions is a business unit of the Altegrity family of companies.

