WHO’S GOT SOMETHING TO HIDE?

SEARCHING FOR INSIDER FRAUD.
About the research

The Annual Global Fraud Survey, commissioned by Kroll and carried out by the Economist Intelligence Unit, polled 901 senior executives worldwide from a broad range of industries and functions in July and August 2013. 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. Almost half (49%) of participants represent companies with annual revenues of over $500m. Respondents this year included 25% from Europe, 24% from North America, 23% from the Asia-Pacific region, 14% from Latin America and 14% 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 ................................................................. 4
Economist Intelligence Unit overview – fraud on the rise .......... 5
The human factor ......................................................... 8
A geographical snapshot .............................................. 10

United States overview ............................................. 12
More people “in the know” spells big cyber troubles .......... 13
Right-sizing your due diligence programs ....................... 14
Independent monitors:
Not just for enforcement actions anymore ...................... 16
Canada overview ...................................................... 18
Brazil overview ......................................................... 19
Who controls the controllers? ....................................... 20
Mexico overview ......................................................... 22
Colombia overview .................................................. 23
Anti-corruption efforts in Latin America:
A changing landscape ................................................. 24
Latin America infrastructure projects
Dealing with the risks .................................................. 26

China overview .......................................................... 28
Pre-empting fraud: Understanding the mind-set of the
Chinese entrepreneur and how business is done in China ...... 29
India overview .......................................................... 31
Investigating procurement fraud in South and Southeast Asia . 32
Malaysia overview ..................................................... 34
Infrastructure investment in developing Asia
Perspectives on risk ..................................................... 35

Europe overview ........................................................ 37
Are you working for a hacker? ........................................ 38
Organized crime infiltration in the supply chain ................. 40
Africa overview ......................................................... 42
Investment in African infrastructure
An opportunity for the private sector ............................... 43
Russia overview ......................................................... 45
The Gulf States overview ............................................. 46

Summary of sector fraud profiles .................................. 47
Contact Kroll .............................................................. back cover

ECONOMIST INTELLIGENCE UNIT REPORT CARDS

TECHNOLOGY, MEDIA & TELECOMS .......................... 15
PROFESSIONAL SERVICES ....................................... 17
MANUFACTURING ................................................... 21
NATURAL RESOURCES ............................................ 25
CONSTRUCTION, ENGINEERING & INFRASTRUCTURE . 27
CONSUMER GOODS ................................................ 30
FINANCIAL SERVICES ............................................ 33
RETAIL, WHOLESALE & DISTRIBUTION .................... 39
TRAVEL, LEISURE & TRANSPORTATION ..................... 41
HEALTHCARE, PHARMACEUTICALS & BIOTECHNOLOGY .... 44
Following a decrease in 2012, fraud is on the rise again, and so are the costs involved in managing it. These factors are in turn driving up companies’ sense of vulnerability. Every kind of fraud covered in this year’s survey saw an increase in incidence, with vendor, supplier or procurement fraud and management conflict of interest seeing the biggest growth.

Awareness of fraud is up, regardless of whether it’s related to cybercrime, information theft, outsourcing or expansion into new and riskier markets. Yet measures to guard against fraud continue to be constrained by budgets and corporate policy.

Particular areas of interest from this year’s report include:

» **The incidence of fraud has increased**
  Overall, 70% of companies reported suffering from at least one type of fraud in the last year.

» **Information-related fraud is common and evolving**
  Information theft affected more than one in five companies over the past year.

» **Fraud remains an inside job**
  Companies that suffered fraud and knew who was responsible reported that 32% had experienced at least one crime where a leading figure was in senior or middle management, 42% where it was a junior employee, and 23% where it was an agent or intermediary.

» **Global modern business practices increase fraud exposure**
  The move to a more global business model that relies on a network of suppliers and partners is leading to a higher risk of fraud.

For the past four decades, Kroll has worked with its clients to help them achieve a deeper understanding of underlying facts in a range of difficult situations and to assist with solutions. Increasingly, fraud exhibits industry-specific and regional characteristics that require detailed knowledge of a market, sector, business process or culture to unearth, redress and prevent. Our global team, on the ground in 45 cities across 28 countries, has the experience and expertise to enable our clients to respond effectively to the ever-changing risk environment.

I hope that this year’s report provides you with some useful insights and helps to identify emerging threats and opportunities for your own business.

Tom Hartley
Chief Executive Officer
For the seventh year running, The Economist Intelligence Unit, commissioned by Kroll, surveyed senior executives from around the world across a wide variety of sectors and functions. This year’s 901 respondents report that fraud remains a widespread problem regardless of the industry or region in which their businesses operate. It is also as protean, and hence unpredictable, as ever. The results of our 2013 report reveal a number of key insights.

1. The incidence and costs of fraud rose markedly in the past year, in turn driving up companies’ sense of vulnerability.

According to this year’s survey, the level of fraud increased by every measure in the past 12 months, reversing recent trends. Overall, 70% of companies reported suffering from at least one type of fraud in the past year, up from 61% in the previous poll. Individual businesses also faced a more diverse range of threats: on average, those hit in the past year suffered 2.3 different types of fraud each, compared with 1.9 in 2012. Finally, the economic cost of these crimes mounted, increasing from an average of 0.9% of revenue to 1.4%, with one in 10 businesses reporting a cost of more than 4% of revenue.

The damage occurred in a wide variety of ways. Every kind of fraud covered in the survey saw an increase in incidence, with vendor, supplier or procurement fraud and management conflict of interest seeing the biggest growth.

The survey offers little hope for relief on the immediate horizon. Of those surveyed, 81% believe that their firm’s exposure to fraud has increased overall in the past 12 months, up from 63% in the previous survey. Respondents attribute this increase to the complexity of information technology (IT) infrastructure, high staff turnover and entry to new, riskier markets.
Just as striking, the share of respondents perceiving a high threat from individual types of fraud has more than doubled in every case. As previous reports have discussed, recent experience with fraud tends to raise feelings of vulnerability, but the sharp growth in the latter this year far outpaces even that of fraud incidence. This suggests that companies are becoming increasingly sensitized to the threats they face and their (sometimes) inadequate protection.

Perhaps the most worrying finding in this year’s survey is that, for six of the 11 types of fraud covered by the survey—corruption, money laundering, regulatory breach, misappropriation of company funds, IP theft and market collusion—the percentage of executives admitting that their firms are highly vulnerable to fraud was higher than the proportion of companies that have been hit in the past year. This indicates that fraud has fertile soil in which to grow.

2. Information-related fraud is common and evolving, but many companies are not prepared for when things go wrong.

Information theft remains the second most common fraud, affecting more than one in five companies over the past year, and three-quarters of respondents describe their businesses as at least moderately vulnerable. Looking ahead, complex IT structures are the most commonly cited reason for an increase in overall fraud exposure (named by 37% of respondents), suggesting that there will be no quick diminution of the threat.

Information theft, like most types of fraud, is typically an inside job: of those hit in the past year in which the attacker is known, 39% say it was the result of employee malfeasance, roughly unchanged from the 37% in last year’s survey. Nevertheless, greater exposure to fraud from IT complexity is being exploited increasingly by outsiders. In this year’s survey, 35% of information theft victims who know the source of the attack report that it was an external hacker, up from 18% in 2012. In addition, 17% of this group suffered as a result of a hacker attack on a vendor or supplier, compared with 5% in the previous survey.

Despite growing concern about information theft and the evolving nature of the threat, preparedness is far from universal. Of those surveyed, 68% say that they currently invest in some sort of IT security, which raises the question of how exposed the other one-third might be.
Looking more closely at these investments, although 66% of respondents say that their firms regularly assess the security of their data and IT infrastructure, only around one-half have a current information security incident response plan [chart 3]. For professional services, the equivalent figures are particularly low, at 51% and 33% respectively, despite sensitive client data being central to many of their activities. Given the breadth of the problem, giving more attention to this area is something worth considering.

3. Fraud remains an inside job, but so does its discovery.

As reported in our earlier surveys, fraud is typically carried out by employees within the company. For the firms that had suffered fraud and the perpetrator was known, 32% had experienced at least one crime where a leading figure was in senior or middle management, 42% in which the incident involved a junior employee, and 23% where it was an agent or intermediary. Similarly, as noted above, employee malfeasance remains the most common driver of information theft. Overall, 72% of those surveyed say that their company has been hit by a fraud involving at least one insider in a leading role, slightly up from 67% last year.

However, this year’s survey also shows that most types of fraud are discovered internally. Management’s discovery of the crime was the most common reason for it coming to light, playing a role 52% of the time when a fraud was exposed, followed closely by internal audits (51%). Only in 10% of such cases did an external audit play a role.

Although senior employee alertness and audits are essential to combating fraud, these mechanisms can be weaker when senior employees themselves are the culprits. For example, according to the survey results, internal audits are slightly less likely to be involved in the uncovering of crime when senior or middle management is involved. Whistle-blowers are therefore an important means to expose wrongdoing. Of those hit by fraud, 32% report that whistle-blowers were responsible for its discovery at their company. More striking, such a tip-off played a role in 41% of the cases in which senior or middle management was involved in the fraud.

Surprisingly few companies, however, are cultivating whistle-blower programs. Only 52% of those surveyed report that they have already invested in staff training about fraud and the creation of whistle-blower hotlines, and just 43% say they intend to increase their investment in this area in the coming year. This may be short-sighted. With most fraud conducted by insiders, helping employees to recognize and report red flags will have clear benefits for companies.

4. Global business practices often increase fraud exposure.

Globalization has changed the way business operates. Companies have for some years now been in search of bigger international markets, while at the same time striving to become leaner. The latter typically involves becoming more focused on areas where they have a strategic advantage and finding ways for others to do the rest through outsourcing or partnerships.

Less appreciated is that these shifts, however profitable, lead to a higher risk of fraud in a variety of ways. For example, 30% of respondents report that entering new, riskier markets has increased their exposure to fraud in the past year. In the same period, greater levels of outsourcing and offshoring raised fraud risk for 28% of those surveyed, and increased collaboration in the form of joint ventures and partnerships for 20%. Overall, 54% of respondents report increased exposure owing to at least one of these factors.

The dangers of new business norms are feeding into other fraud figures. Of the companies that were hit in the past year and where the perpetrator was known, 30% suffered at the hands of vendors or suppliers and 11% at those of their joint venture partners. Similarly, procurement fraud was the fourth most common type of those covered in the survey this year (19%) and saw the biggest increase compared with last year.

Given the high level of risk, a surprisingly small proportion of companies are taking action. Only 43% intend to invest in greater due diligence for partners or vendors over the next 12 months. One of the reasons may be that, in the search to reduce costs—a permanent feature of global competition—fraud prevention can get left to the side. 20% of respondents report that a lack of resources or an insufficient budget to support compliance infrastructure is increasing their exposure to fraud. Companies need to be prepared for the dangers of fraudsters operating in the same global marketplace as they do.

5. Those with local knowledge see fraud risks everywhere.

Certain regions have a reputation for high levels of fraud. It comes as no surprise, therefore, that 13% of all respondents were dissuaded in the past year from operating in Africa, and 11% in Latin America, from their experience or perception of fraud.

More striking is the degree to which fraud is keeping companies from making local investments, even in regions where the problem is thought to be relatively well controlled, particularly North America. Even in a globalized world, companies typically invest closer to home. These figures therefore suggest that both the existence or appearance of fraud is a substantial drag on possible new investment and that outsiders coming in need to be aware of risks even in regions with a reputation for low levels of fraud.
The Human Factor

By Tommy Helsby
Economies are growing again. 
Stock markets are booming. 
Big deals are closing. 
And the fraud statistics are back on the rise. 
It’s as if the financial crisis never happened.

Well, not quite. Regulatory pressure shows no sign of disappearing – in a separate survey of general counsels we have just completed, it was clearly the prime issue on people’s agenda, and is driving a significant growth in compliance activity. This is probably driving increased fraud awareness – and fraud detection, given that we also see a rise in companies reporting that they have victims of fraud. Undiscovered and unreported fraud, however minor, is an infection with the potential to grow into a life-threatening corporate disease – just read the stories of Enron, Satyam, Madoff, Parmalat and other major scandals, each of which started with small frauds that grew to consume the business.

It is noteworthy that awareness of the vulnerability to insider crime has shown particular growth.

Regulatory breach, conflict of interest and market collusion are all classic inside jobs, and the Global Fraud Survey results show a tripling of the number of companies being aware that they are “highly vulnerable,” an awareness that is driving and being driven by the growth of the compliance function.

This has been a theme in many previous Kroll Fraud Reports and it is encouraging that the message is being received more broadly.

Increased regulation is not the only change. Much of the financial recovery is being led by government spending; not only quantitative easing but massive investment in infrastructure projects – one estimate suggests an average of $4 trillion per year over the next 15 years. Even when it is not government funded, infrastructure investment involves heavy interaction with government, for licensing, planning and coordination. It is also disproportionately focused on emerging markets, which have the greatest need of development; and typically, it involves joint ventures and local partners. When you look at this from a fraud-risk perspective, it’s a high stakes trifecta: government contracts, emerging market exposure and third party agents, each one of which is identified by our survey participants as an area of concern.

So, one of our themes in this year’s Fraud Report is infrastructure. Our experience in this area shows the global nature of the sector – Japanese companies investing in South America, Chinese and European companies competing in Africa and so on. But this should not distract from the equally damaging local problems: I can think of many examples of fraud cases involving a company operating in a single country suffering real damage from a crooked procurement or contracts manager. The impact is often not just financial, but costs management time, morale and reputation.

Our second big theme this year centers around one of the other major changes since our first Fraud Report in 2007: the rise of cyber fraud.

Computer-related crime is certainly not new – we have been active in this area for over 25 years. But the scale of the threat is new, and as an ever greater proportion of business activity becomes digital, the potential for economic and commercial damage grows with it. Every day brings a report of a new incident, with victims including companies in every sector and size, together with government agencies, charities, universities, hospitals and NGOs.

Clearly, awareness of the problem has grown rapidly, especially in the media. But there is still too much focus on the threat from 5,000 miles away rather than the man in the next office. It is perhaps more comforting to think of the enemy as a faceless hacker in a distant land; but our experience shows that to be the exception rather than the rule.

The greatest vulnerability is a careless, vengeful or malicious employee, who has already got past most of your defenses by virtue of being an employee (or often, an IT contractor). Equally, your best defense may be another employee, who spots the aberrant behavior and has been encouraged to alert management on a timely basis. The human dimension to cyber fraud is often overlooked.

Indeed, the human dimension to fraud in general is central to Kroll’s work. Cyber investigation tools, forensic analysis of books and records and open-source data research are all critical tools in our arsenal, and our use of them is second to none. But the most valuable tool is the experience of human nature gained through years of investigation, and cultural understanding of what to expect and what to look for in different regions around the globe. This connects with one further change: the inexorable spread of globalization.

The fraud case involving a single location is now a rarity: the client is in one country, the fraud in a second, the perpetrator in a third and the money…well, that’s often the challenge.

But without a good understanding of how things work in each place, that’s a challenge that may not be fully met.

Tommy Helsby is Chairman of Kroll, 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.
We compared the results of the Global Fraud Survey with Transparency International’s Corruption Perceptions Index (CPI). The CPI measures 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 2012

<table>
<thead>
<tr>
<th>SCORE</th>
<th>Cleanliness</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.0 - 10.0</td>
<td>Very Clean</td>
</tr>
<tr>
<td>8.0 - 8.9</td>
<td>Very Clean</td>
</tr>
<tr>
<td>7.0 - 7.9</td>
<td>Very Clean</td>
</tr>
<tr>
<td>6.0 - 6.9</td>
<td>Very Clean</td>
</tr>
<tr>
<td>5.0 - 5.9</td>
<td>Very Clean</td>
</tr>
<tr>
<td>4.0 - 4.9</td>
<td>Very Clean</td>
</tr>
<tr>
<td>3.0 - 3.9</td>
<td>Very Clean</td>
</tr>
<tr>
<td>2.0 - 2.9</td>
<td>Very Clean</td>
</tr>
<tr>
<td>1.0 - 1.9</td>
<td>Very Corrupt</td>
</tr>
<tr>
<td>0.0 - 0.9</td>
<td>Highly Corrupt</td>
</tr>
<tr>
<td>No data</td>
<td>Highly Corrupt</td>
</tr>
</tbody>
</table>

Fraud at a glance

Transparency International’s Global Fraud Survey with Kroll

Frequently go hand in hand.

The comparison clearly demonstrates that fraud and corruption levels of public sector corruption, as seen by business people and country analysts, ranging between 10 (very clean) and 0 (highly corrupt).

The CPI measures 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.

A geographical snapshot

We compared the results of the Global Fraud Survey with Transparency International’s Corruption Perceptions Index (CPI). The CPI measures 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.
Management

Europe has a growing fraud problem. Overall, fraudsters hit 73% of businesses at least once during the last year, which is slightly above the survey average (70%). Moreover, for all but one individual fraud covered in the survey, the European incidence was within 2.5% of the global figure. The sole exception was information theft, which was slightly more common on the continent (25%) than overall (22%).

The proportion of those reporting an increase in fraud exposure at their firms has grown from 69% in the 2012 survey to 80% this time. Moreover the sense of vulnerability in China towards conflicts of interest, vendor or procurement fraud, IP theft and regulatory or compliance breach has grown dramatically.

THE GULF STATES
72% of companies in the Gulf suffered at least one incidence of fraud – slightly above the global average, but the increase from 2012 of 49% was more than twice as great as that experienced in the rest of the world. Gulf States currently have the highest regional incidence of information theft (31%), vendor or procurement fraud (35%), market collusion (28%), and management conflict of interest (24%).

Malaysian respondents are more likely than average to report that vendors were leading parties.

Corruption and bribery 30%
Management conflict of interest 21%
Regulatory or compliance breach 21%

Two types of fraud are worryingly widespread in Malaysia - theft of physical assets and vendor or procurement fraud. Where the perpetrator was known, Malaysian respondents are more likely than average to report that vendors were leading parties.

Over the last 12 months the country had an above average incidence of theft of physical assets, corruption, internal financial fraud and information theft. Insider fraud is particularly rife in India, 89% of respondents indicated that the perpetrator was an insider of some sort – a junior, middle management, or senior employee or an agent.

 adam@FraUD.HTto-a.naGL.png

Fraud at a Glance

Prevalence

73%

Prevalence

72%

Prevalence

69%

Prevalence

67%

Prevalence

66%
**UNIVERSAL STATES OVERVIEW**

The United States has an incidence of fraud below the overall average – 66% of companies were hit by one fraud in the last year compared to 70% globally – and a rate of loss that is also slightly under the norm – 1.2% compared to 1.4% for the survey as a whole.

Nevertheless, the situation is far from ideal. For eight of the 11 frauds covered in the survey, the reported incidence within the United States is within 2% of the global mean. Moreover, significant increases in the past year have taken place in the prevalence of management conflict of interest (21% of respondents’ companies were affected compared to 16% in the 2012 survey), regulatory and compliance fraud (17% up from 7%), IP theft (12% up from 8%), and money laundering (5% up from 1%).

Even some of this year’s good news might not last. Although the incidence of information theft declined from 26% in the 2012 survey to 20% this year, 23% of respondents say that they are highly vulnerable to this crime, up from just 7% last year, perhaps because IT complexity is the leading cause of increased exposure to fraud risk, affecting 44% of respondents’ companies.

The biggest danger, though, appears to be complacency. As in the past, US companies are less likely than average to be planning further investments in every one of the anti-fraud strategies covered in the survey. In a majority of cases, they are also less likely to have these protections in place. Financial controls constitute the clearest example: 64% of American respondents say their firm has them already and 32% plan to invest further. The global figures, on the other hand, are 71% and 44% respectively. Companies in the United States will need to be more active if they want to keep fraud levels as low as in the past.

<table>
<thead>
<tr>
<th>Prevalence: Companies affected by fraud</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management conflict of interest (21%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information theft, loss or attack (20%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Theft of physical assets or stock (20%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory or compliance breach (17%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information theft, loss or attack (26%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Theft of physical assets or stock (24%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management conflict of interest (16%)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Increase in Exposure: Companies where exposure to fraud has increased</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT complexity (44%)</td>
<td></td>
<td>IT complexity (35%)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Loss: Average percentage of revenue lost to fraud</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2%</td>
<td></td>
<td>1.1%</td>
</tr>
</tbody>
</table>
More people “in the know” spells big cyber troubles

By Timothy P. Ryan

Knowledge is the fuel that drives much in today’s global economies – from industrial formulas and know-how, to science pushing both nano and stellar frontiers, to the specialized expertise of diverse professional services firms for virtually every human endeavor.

For many companies, success in a number of areas hinges on continually expanding and sharing that knowledge within the enterprise, not to mention employing the most efficient ways to facilitate that sharing. However, this does not bode well when it comes to cyber security. In Kroll’s experience assisting clients across diverse industries, the greatest threat to an organization’s cyber security is the insider.

As companies allow their people to be “in the know,” with access to intellectual property (IP), confidential information and client-specific data, they inherently leave themselves open to theft by these same insiders. While the threat is pervasive, Kroll has found that companies are most vulnerable in three particular areas.

1. H1B visa workers: When they go back, what will they take with them?

In the pursuit for technically trained professionals to work on their projects, many organizations turn to non-citizen workers on H1B visas to fill knowledge gaps in their employee workforce. The practice is well-established in the industrial and technology sectors, which often derive the added benefit of an outsider’s culturally different perspective. Visas are for a finite duration, however, and companies must be prepared for two eventualities: When workers return to their native countries, what might they take with them? And if they do, what practical recourse does an employer really have?

If companies perform any background checks on these workers, and we find that many do not, checks are often limited in scope to educational verifications. Compounding the problem is that customary legal instruments and remedies that can be enforced domestically, such as nondisclosure and non-compete agreements, are effectively meaningless once a worker has returned to his or her native land. If litigation is even a possibility, it is sure to be a protracted and expensive fight, with no guarantees that damages can actually be collected.

2. Independent contractors and temps: Here today, gone tomorrow with your IP?

Like their H1B visa worker counterparts, independent contractors and temporary employees are increasingly being used by companies for strategic staffing purposes. Whether a company needs to supplement a short-term need for expertise or deal with fluctuating business volumes, the use of these workers has delivered both operational and financial efficiencies. Once again, however, a company should be prepared for a two-fold risk.

First, contractors and temps must often be exposed to valuable business information and given access to company systems. Second, and a much more difficult and thorny dilemma to contend with, is that an independent contractor’s most valuable competitive advantage is the knowledge and experience that he or she is able to bring to a client. The ability to rely on and access data or processes that were developed on a previous engagement may prove the deciding factor in landing a new client.

Which brings up another similarity with H1B workers – all these workers usually know exactly when an engagement or project will be over. Impending stressors, e.g., the loss of a job, have long been recognized as triggers for both physical and cyber thefts. It’s not surprising, then, why these categories of workers can be problematic elements in any cyber security equation.

3. Remote employees: What’s accessed at home stays at home?

Technological advancements in both software and hardware have vastly multiplied how and where employees can carry out their responsibilities. From an employer’s perspective, the sea change has proved a boon in several ways, both tangible and intangible. Aside from lowering their capital costs, companies have seen improvements not only in worker productivity but also in being able to recruit top candidates and/or retain high-performing employees virtually anywhere in the world. However, the same technology that facilitates access from multiple devices to a company’s systems and data can leave the door open for at best, misguided efforts to back up work, and at worst, malicious tampering or outright theft.

For all intents and purposes, not only are remote workers not subject to the multiple layers of security measures that might be enforced in a physical location – they also often do not encounter significant impediments in how they access, retain, and store company data on their personal devices.

Recognize the risk from those in the know and manage accordingly

If knowledge is the lifeblood of many businesses today, H1B workers, independent contractors and temps, and remote employees can be the source of internal losses that go undetected until it’s too late. However, the risks posed by each of these groups can be managed. From our experience, Kroll recommends these best practices:

1. Identify and contain sensitive data.
2. Screen independent contractors and temporary workers the same as you do employees.
3. Encrypt or limit the use of remote devices.
4. Establish and enforce consequences for security violations.
5. Engage conflict-free examiners to conduct investigations on malicious insiders who abuse IT systems.
6. Centralize and safeguard computer logs of important IT systems in a restricted-access location.
7. Establish thorough employee termination procedures.
8. Restrict the use of removable media.
9. Run and require acceptance of terms on privacy banners.
10. Back up data.

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.
This year’s survey findings justify their concerns. For companies actually affected by fraud, the category with the biggest jump was in vendor/supplier/procurement relationships – up from last year’s 12% to 19% now. When nearly one in five companies is experiencing fraud in this area, investing in the right due diligence can save millions of dollars and countless management man-hours negotiating opportunities and avoiding pitfalls.

While the problem is widespread, and depending on the jurisdiction seemingly intractable, many of Kroll’s clients are experiencing positive results with a three-pronged approach:

» Management setting the tone from the top with a commitment to a strong compliance ethic
» Creating and maintaining a robust compliance program
» Conducting appropriate levels of due diligence that are commensurate with the scope of the transaction and jurisdictional transparency

Commitment to compliance must come from the top. A strong commitment to compliance, driven by the company’s senior management, is key for reinforcing an environment that helps employees stay focused on operating ethically. It also creates the expectation that all new ventures receive an appropriate level of due diligence review.

Robust compliance programs standardize procedures. In addition to setting the tone from the top, organizations also need a robust compliance program that ensures a standardized process is undertaken at all levels and subsidiaries of the company. This is especially critical for when new agents, joint venture partners, vendors, suppliers or other third parties are brought into the corporate fold. At a bare minimum, the program should encompass some basic due diligence as well as components that confirm each relevant person’s awareness and assurance of a commitment to follow the company’s ethics and compliance policies and procedures.

Right-sizing due diligence efforts can pay off in the long-term. For significant commitments to new ventures, however, more comprehensive investigative due diligence may be necessary. This is often true in jurisdictions where corruption and bribery are prevalent in the conduct of business. Exactly whom is the company interacting with to get the deal done? Are there government officials involved and in what capacity? This has been a particular area of SEC and DOJ interest over the last couple of years, with sizeable fines for payments of bribes by subsidiaries to government officials. Just in 2013, these fines have topped $400 million. Particularly in countries where the availability of public records is thin, boots-on-the-ground reputational inquiries are often the only way to ascertain relationships held by the agents/third parties and their ability to bring the deal to fruition as they claim, in an appropriate manner.

How much due diligence is needed?

That is the million-dollar, unanswered question. The short answer is: It depends. The US Securities Act of 1933, the Foreign Corrupt Practices Act, UK Bribery Act and other regulatory acts don’t specifically define the level of due diligence required. Instead, they use words like “robust,” “appropriate,” “enhanced” and “adequate.” In essence, regulators seem to want to ensure that parties find any potential problem. For example, if a material issue is not identified, the authorities could arguably question whether the level of due diligence was appropriate.
The technology, media and communications industry had an unusual pair of results in this year’s survey: although it had one of the lowest overall incidences of fraud, with only 66% of companies hit, it also had the highest average fraud loss as a proportion of revenue (1.8%). It has helped to drive up costs has been the most widespread problem with information theft, loss or attack in any sector (31%). The issue is not merely one of weak technological defenses, although IT complexity is a driver of increased fraud risk at 37% of the companies surveyed. Industry companies are more likely, on average, to be investing further in security software as well as specialized and general staff training, an effective defense should include greater physical protection of technological assets.

The main difference in the source of information theft between this sector and the survey average is a much higher level of theft of physical devices from companies or employees. This was involved in one-half of cases of information theft and is the most common mode of attack against companies within this sector. With only 35% of firms in this industry investing in physical asset security in the coming year—far below the overall survey average of 44%—this problem may continue to undermine information security efforts elsewhere.

Certainly in jurisdictions with less transparency, where the availability of public records is slim or non-existent, where independent media is censored/restricted, or where corruption and bribery are common ways of doing business, more comprehensive due diligence is advisable. Particularly in these instances, the due diligence should follow a more rigorous investigative methodology rather than the more simple screening regimen. This involves an iterative research process, challenging data found and re-researching findings and conducting analysis to fully understand the implications of those results. Combined with local source inquiries of knowledgeable resources, these efforts can help a client feel more comfortable about the level of understanding they have with regard to their business partners and third parties.

On a recent joint venture relationship opportunity in the Middle East, the client asked Kroll to conduct investigative due diligence into the principals of the company. Our research quickly started identifying flags about the subjects, including the fact that their bios, word for word, were identical to the bio of other individuals involved in the same line of business in Dubai—only the names were different. The website for the company had only been formed a couple of years ago, odd for a company with 18+ years in business. Worse, we found that the registrant of the website was linked to a known Nigerian fraudster. Needless to say, the client ran from the potential relationship. But it took this investigative level of insight to identify issues that might have otherwise slipped through lighter levels of inquiry.

So, perhaps, the answer to the million-dollar question isn’t a predetermined level of due diligence. Rather, companies should instead focus on compliance programs designed with elements that can raise red flags and identify problems, then escalate due diligence as necessary to deliver the most effective protection and confidence in their new deals.

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.
Independent monitors: Not just for enforcement actions anymore

Enhanced government scrutiny in the global regulatory environment has incentivized companies to strengthen their anti-money laundering and anti-corruption practices. Penalties are increasing, with exposure for violations under the Foreign Corrupt Practices Act (“FCPA”) and other laws and regulations in some cases running upwards of hundreds of millions of dollars. The consequences of non-compliance are not only monetary; associated negative publicity can also severely damage a company’s reputation and decrease its ability to do business.

By Dan Schorr and Emily Low

FCPA enforcement actions are usually resolved through deferred prosecution agreements and non-prosecution agreements, which often impose an independent monitor to ensure the company’s previous failures are not repeated and that adequate safeguards are put in place to ensure compliance with Bank Secrecy Act (“BSA”) and anti-money laundering requirements. Such monitors are becoming increasingly utilized at the federal, state and even local level of government.

**Effective compliance requires focus on implementation and enforcement**

Although companies may have a compliance structure in place, such existing intended safeguards are often inadequate: Employees need to be trained on compliance with the FCPA, reporting structures must be properly aligned, and the system of internal financial controls needs to be audited and periodically re-assessed and re-evaluated. FCPA anti-bribery provisions, as well as the books and records and internal control requirements, necessitate very specific training. An appropriate external monitor already has the team infrastructure, skills and expertise to provide education; track expense reports and transactions; audit financials; and impose controls necessary to prevent, deter and detect improper payments.

Companies frequently do not have adequate internal controls to ensure compliance with applicable policies, procedures and practices. Even if such controls do exist, they are often unenforced. According to a separate survey conducted for Kroll’s recent Anti-Bribery and
The utilization of monitors is becoming more common in the construction industry. For example, a major US city decided the best course of action was for the general contractor on certain construction projects to designate a small percentage of the contract price for a monitor to help prevent safety violations, abuse of workers or other violation of law on-site. Less than 1% of the contract price is set aside to ensure compliance with construction, banking, anti-money laundering, safety and environmental laws and regulations. For that relatively small cost of having an independent monitor on-site, the benefit to the City and the general contractors is significant.

An appropriate external monitor will be in a good position to prevent FCPA violations, construction fraud, labor law violations and other legal and financial exposure. Monitors can provide an independent assessment and are often better suited than an internal compliance department to develop, implement, test, analyze and improve the compliance controls and programs in place, in addition to identifying and addressing areas of non-compliance. It is important to take proactive measures to address FCPA, BSA and other legal compliance and potential fraud. If a company is cited for FCPA or other violations, having had an effective compliance program will often reduce the ultimate penalties.

Safeguards must go beyond reliance on internal controls

Companies that think their internal audit teams are an adequate safeguard need to look no further than one major financial company, which agreed to pay a nine-figure sum to hire a corporate compliance monitor to assist with implementing measures to address FCPA, BSA and other legal compliance and potential fraud, financial reviews, asset searches and cases related to international business intelligence. In Asia, Kroll led an FCPA compliance review on an acquisition target for a dual Hong Kong and US-listed company. Kroll’s investigation and review led to the implementation of a comprehensive compliance program.

Independent monitors play key role for ongoing and future compliance

As recently as May 2013, the Securities and Exchange Commission (“SEC”) charged a European company with FCPA violations of bribing intermediaries of a foreign government official to obtain contracts. The company agreed to a very significant payment to settle the SEC and criminal charges and to hire a corporate compliance monitor to assist with implementing and testing a compliance and ethics program.

As recently as May 2013, the Securities and Exchange Commission (“SEC”) charged a European company with FCPA violations of bribing intermediaries of a foreign government official to obtain contracts. The company agreed to a very significant payment to settle the SEC and criminal charges and to hire a corporate compliance monitor to assist with implementing and testing a compliance and ethics program.

Corruption and bribery

Theft of physical assets or stock

Money laundering

Regulatory or compliance breach

Internal financial fraud or theft

Misappropriation of company funds

Information theft, loss or attack

IP theft, piracy or counterfeiting

Vendor, supplier or procurement fraud

Management conflict of interest

Market collusion

Loss: Average percentage of revenue lost to fraud: 1.4%

Prevalence: Companies affected by fraud: 65%

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

Management conflict of interest (22%) • Theft of physical assets or stock (15%) • Information theft, loss or attack (14%)

Increase in Exposure: Companies where exposure to fraud has increased: 73%

Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected: N1 complexity (34%)
In previous years, Canadian survey respondents have often reported overall fraud incidence well below the global average. This time around the news is more negative: 69% of Canadian companies were affected by at least one fraud in the last year – very close to the survey average (70%).

Canada’s fraud picture, however, differs markedly from the global norm. In some areas – such as vendor or procurement fraud, internal financial fraud and market collusion – those surveyed report incidences well below that in other parts of the world. For two frauds, though, Canadian companies have much larger problems than their peers: the country’s incidence of management conflict of interest (29%) was the second highest of any geography in the survey and that for information theft (29%) was also one of the highest and well above the survey average (22%). These types of fraud tend to be expensive and it shows, as Canadian respondents’ companies lost 1.7% of revenues to fraud last year, compared to a global average of 1.4%. Moreover, as the ongoing Quebec corruption inquiry demonstrates, the country is not immune to this fraud. Its reported incidence this year (14%) was the same as that for the overall survey.

Given the high level of management conflict of interest, it is not surprising that this year senior managers were frequently among those illegally taking money from firms. Of those companies which experienced fraud in the last year and where the perpetrator is known, senior or middle managers played a leading role at 43%, well above the survey average of 32%.

Surprisingly, Canadian companies are less active than most in protecting themselves against their biggest fraud problems: only 63% are putting money into new IT security software in the next 12 months, compared to 68% on average. More striking, just 29% have tested an information security incident preparedness plan in the last six months, compared to 48% on average. Similarly, only 40% are investing further in management controls, compared to 43% for the survey as a whole. Finally, just 34% are putting money into staff training and whistle-blower hotlines (the latter often proving a good source of information on middle and senior management fraud), compared to 43% on average. Canadian firms will have to try harder in order to address their big problems better.
Brazil’s fraud problem grew faster than that of the rest of the world over the past 12 months. Seventy-four percent of those surveyed in the country report that their companies were affected by at least one fraud in the last year (up from 54% in 2012) and businesses on average lost 1.7% of revenues to such crimes (up from 0.5%). Brazil also had the highest incidence of theft of physical assets (37%) of any region or country covered in detail in the survey outside of Africa, as well as above-average rates of management conflict of interest (26% compared to 20% overall) and vendor or procurement fraud (23% compared to 19% overall).

Looking ahead, Brazilian respondents are also likely to see a high risk of fraud growing in the future. Over three-quarters consider their firms at least moderately vulnerable to seven different frauds: corruption (93%), vendor or procurement fraud (93%), IP theft (88%), theft of physical assets (86%), information theft (84%), management conflict of interest (79%), and regulatory/compliance breach (79%). Moreover, 86% say that their exposure to fraud has increased, with high staff turnover (42%) and complex IT (40%) common reasons.

These concerns, though, are not necessarily driving investment. For every anti-fraud strategy covered in the survey, Brazilian companies are only about as likely to be planning investments in the next year as the overall survey average. Worse still, too many companies are practicing false economy: 30% say that one driver of increased fraud exposure has been lack of budget or resources for compliance infrastructure.
Who controls the controllers?

By Matías Nahón

In Argentina, growing companies can suffer great losses due to negligence – often unintentionally – when high-level executives fail to establish and regularly revisit and adjust the necessary internal controls.

Many corporate frauds aimed at evading a company’s internal controls in order to misappropriate cash, information, goods or intellectual property are crimes that could be thwarted if companies would allocate sufficient time and money for fraud prevention planning.

Despite this, an increasing number of companies in Argentina and elsewhere in the region have either not invested in fraud prevention programs or have failed to adjust existing internal controls to cope with their firm’s rapid growth. These are complex organizations – with more production, more sales, and a greater number of suppliers – yet they are reluctant to ensure that the sophistication and scope of their internal structures match the level of their operations. Consequently, this failure to upgrade and adjust results in managers becoming overwhelmed by their duties and internal control responsibilities, with no time or resources to master the multitasking demanded of them.

Many areas in the company may become “Free Fraud Zones.” Such zones are areas that allow fraud to occur unchecked – where the controller may become a key participant in the scheme to defraud as an accomplice who does not apply or enforce controls. In our experience, we are seeing two major forces at work causing this type of “fraud by omission” to increase year over year in Argentina:

**Corporate cost reduction strategies expand responsibilities but decrease resources for managers with control duties.**

Cost reduction policies are frequently applied to different company departments, and certainly the practice does not occur only in emerging markets. However, it seems to be common for the companies involved in this kind of market to allocate less than the necessary resources to management positions related to control. In our experience, we especially see this with companies that operate in the “Southern Cone” countries, which are often considered “one great country” by multinational companies in Latin America. In many instances, when companies expand their operations in the region, they give their executives responsibilities over a larger area, but they must do so with almost the same resources they had when leading a much smaller area. In essence, local positions become regional positions.

Who controls the controllers?
Because executives often find themselves unable to decline the “promotion,” companies generate the ideal scenario for corruption or fraud to flourish when they do not recognize or accept the greater stress being placed on these managers as well as the greater span of control that needs increased support from adequate fraud prevention programs.

For example, Kroll recently worked on a fraud case for a major multinational food company operating in Argentina, Uruguay and Brazil. Even after experiencing significant growth in its exports and production, the company still had only one regional manager to oversee and control activities in all three countries, and one area retail manager with responsibility for sales to many regional retailers. Our research showed that although only one party had the intention to commit fraud, there were three facilitators of the crime: (a) the fraudster, who instead of reporting company vulnerabilities intentionally took advantage of them and committed the crime; (b) the regional manager, who did not fulfill his internal control duties; and (c) the company itself, for not investing in human resources and more effective fraud controls.

Economic policies – such as replacing imported goods with local products – boost the number and size of transactions for many small and medium local companies.

Argentina is a prime example of how rapid growth in a country sets the stage for companies to realize not only great opportunities, but also significant internal control challenges. According to official data, Argentina’s Gross Domestic Product (GDP) grew over 30% in the last 6 years. Industries in the region are not only addressing the growing demands of these larger domestic markets, but also engaging in export markets. However, many of these domestic companies do not have the mechanisms for – or even recognize the need for – appropriate fraud control measures that are adjusted for the company’s new operational dimensions. Major deficits in fraud control systems can then occur, with the result that these market “opportunities” bring with them a significant risk for fraud.

In this kind of high-growth scenario, increasing responsibilities are usually delegated to the same executives.

Management on the ground, who are having difficulties dealing with growing operational and commercial challenges, have little time to spare for adjusting or instituting new preventative fraud control measures. This creates a fertile environment and opportunity for fraud to begin.

Where previously a direct line for the crime could be traced back to the bad intentions of the fraudster, now the seeds of fraud can be found in the lack of corporate fraud controls, negligence on the part of high-level executives, and the company’s own inadequate human resource investment in qualified staff focused on fraud prevention.

The time has come to support companies in this challenge. It is impossible to overstate the value of preventative actions that include background and reputation checks on executives, as well as a comprehensive assessment of operational vulnerabilities. The results of both can raise red flags for potential fraud while also providing a roadmap for ways to prevent gaps in the fraud prevention infrastructure and to neutralize distractions for relevant management and controllers before they can cause multimillion-dollar losses.

Interpreting this year’s survey for manufacturers is a matter of perspective. On the positive side, after exceptionally poor results in 2012, the sector is the only one to see a marked decrease in the overall incidence of fraud (from 87% to 75%) and in average revenue lost to fraud (from 1.9% to 1.6%). Compared with other industries, however, the results remain disappointing. Manufacturing still had the highest overall incidence of fraud and the second greatest rate of revenue lost to fraud in the survey. Moreover, it had the second highest incidence of theft of physical assets of any industry (44%) and the highest frequency of intellectual property theft (14%). Finally, the sector is particularly prone to insiders seeking dishonest gain: 54% of known frauds in the past year involved junior employees in a leading role. More broadly, 56% of all manufacturers suffered fraud at the hands of an employee or an agent, rising to 77% for companies hit by fraud where the perpetrator was known.

The most worrying aspect of the results is that manufacturers are excessively accentuating the positive. For all but three types of fraud, manufacturing sector respondents are less likely, on average, to see their companies as at least moderately vulnerable, and for the exceptions the difference from the survey median is only slight. Similarly, for nine of the 10 anti-fraud strategies covered in the survey, manufacturers are only about as likely as, or less likely than, the average to be contemplating investment in the next year. Worse still, 30% say that they simply lack the budget or resources for compliance initiatives. Even with some improvement over the past few years, fraud levels in the manufacturing sector remain much too high for the industry to rest on its laurels.

| Percentage of firms reporting loss to this type of fraud: 1.6% |
| Loss: Average percentage of revenue lost to fraud: 1.6% |
| Prevalence: Companies affected by fraud: 75% |
| Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud: Theft of physical assets or stock (44%) • Vendor, supplier or procurement fraud (20%) • Information theft, loss or attack (19%) • Regulatory or compliance breach (18%) • Management conflict of interest (15%) |
| Increase in Exposures: Companies where exposure to fraud has increased: 85% |
| Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected: Entry into new, riskier markets (40%) |
The incidence of a wide number of frauds saw substantial growth in Mexico over the last 12 months, including theft of physical assets (30% of respondents based in the country report their company being affected, up from 19% in the 2012 survey), internal financial fraud (25% up from just 7%), corruption and bribery (25% up from 15%), vendor or procurement fraud (23% up from 19%), and regulatory or compliance fraud (20% up from 4%).

Outside of sub-Saharan Africa, the internal financial fraud figure was the highest for any region or country looked at in detail by the survey. Just as alarming, the financial loss to fraud more than doubled from 0.7% in the 2012 survey – well below that year’s overall average – to 1.9% this time around – well above the global norm.

Meanwhile, risk is growing rapidly: the number of respondents saying that their company had become more exposed to fraud in the last 12 months went from 56% in the 2012 survey to 93% this year – the highest figure for any country or region in 2013. High staff turnover alone is increasing the danger at almost half of companies (45%). Growing IT complexity (40%), entry into new markets (40%), increased outsourcing (35%) and increased collaboration (33%) are also widespread sources of greater exposure. As a result, 20% or more of those surveyed regard their businesses as highly vulnerable to every fraud covered in the survey, except for management conflict of interest and internal financial fraud where, in both cases, 18% still do.

Despite the rapid growth in vulnerability, though, too many companies are unwilling to invest in protecting themselves: 38% report a lack of budget for compliance infrastructure, another survey high. If Mexican fraud figures are not to keep rising, companies will need to be aggressive in tackling the heightened risk.
Like last year, 2013 survey respondents from Colombia report that the country’s fraud problem is smaller than the global norm: just 63% of businesses were affected by at least one fraud in the last 12 months and the average loss to fraud (0.7%) is well below the survey mean (1.4%).

On the other hand, the figures show a rapid rise in fraud. In the 2012 survey, the overall incidence of fraud was only 49% and the average loss just 0.4%. Similarly, in the 2012 poll, only two frauds were more common in Colombia than in the survey as a whole, but this year it is four – theft of physical assets (37% compared to 19%); vendor or procurement fraud (20% compared to 19%), corruption (17% compared to 14%), and market collusion (13% compared to 8%).

Looking ahead, things have the potential to grow worse: a striking 90% of respondents say that their exposure to fraud has increased in the last year, roughly double the 46% who reported this in the 2012 survey. Nearly half of those surveyed in Colombia this year (47%) say that high staff turnover is a driver of higher fraud risk, and the same number say the same thing about entry into new markets.

The data show that a substantial number of Colombian firms will be making additional investments in a range of anti-fraud strategies, but also indicate that at 27% a lack of budget is constraining this in at least some cases. In the current environment, these companies cannot rely on the previously low incidence of fraud to keep them safe.
The passage of these regional laws coincides with increased scrutiny on business transactions in Latin America by the US DOJ and the US SEC. In recent months, actions concerning Foreign Corrupt Practices Act (FCPA) violations have been brought against companies and individuals doing business in Argentina, Brazil, Mexico, Panama, and Venezuela. Moreover, an increase in future Latin American-focused FCPA cases is likely, as the risk and prevalence of corruption remains high, and the new local anti-bribery laws set the expectation for more effective judicial cooperation between the US and Latin America.

Brazil
After millions took to the streets in more than 100 Brazilian cities in June-July 2013 to express discontent over their government’s massive public spending and lack of institutional transparency, Brazilian politicians were spurred into passing a landmark anti-corruption bill that had previously stalled in Congress for over three years. Known as the “Clean Company Law (Lei Anticorrupção Empresarial),” the legislation establishes direct civil and administrative liability for companies found guilty of foreign and domestic bribery and takes effect in January 2014. The new law includes harsh penalties for violations, and gives the government authority, among several remedies, to seize a company’s assets or blacklist it from future contracts.

Colombia
Colombia, the Andean region’s most populous country, has undertaken significant efforts to fight corruption. The new Anti-Corruption Statute (Law No. 1474 of 2011) criminalizes the bribery of both local and foreign public officials, includes imprisonment penalties of up to 15 years and, like the UK Bribery Act, specifically addresses commercial bribery. A significant development is the launch by President Juan Manuel Santos of the world’s first “High Level Reporting Mechanism” (HLRM) in April 2013. The HLRM is a preventive mechanism designed to address corruption in public procurement and the public sector, to issue early warnings and allow the government to take necessary corrective measures but, at the same time and to the extent possible, ensure that the bidding procedure is successfully carried out.

Latin America’s long-awaited broad-scale mobilization against corruption has started to materialize, and is expected to continue. Due to popular demands from a growing middle class as well as pressure from international development organizations, countries such as Brazil, Colombia and Mexico have recently enacted anti-corruption frameworks that place strict penalties on individuals and corporations found guilty of acts of bribery, fraud in public procurement and bid rigging.
Mexico

Mexico has also seen corruption move to the forefront of public concern. Shortly after becoming President-Elect in late 2012, Enrique Peña Nieto announced a bill to create a National Anti-corruption Commission that would have the powers to investigate both private and public corruption cases at federal, state, and municipal levels.

A few months earlier, the Federal Law against Corruption for Public Procurement (Ley Federal Anticorrupción en Contrataciones Públicas – LFACP) went into effect in June 2012. The LFACP could play an important role in developing the necessary institutional reform to handle President Peña Nieto’s plans to allow private investment in Mexico’s oil and gas sector for the first time since 1960, which could usher in a wave of new foreign direct investment.

Enforcement challenges

Policy experts have identified a significant correlation between corruption and the strength of a nation’s regulatory and enforcement mechanisms. Countries such as Haiti and Venezuela, which have among the lowest international rankings of public governance, correspondingly have the highest rates of perceived corruption. Conversely, Chile, which has the strongest institutional controls according to the 2013 World Bank “Doing Business Report,” also maintains the Latin America’s lowest rate in fraud, bribery, and graft.

As Chile’s success in combating corruption has demonstrated, the challenge for Latin America has less to do with enacting policy and more to do with implementing and enforcing it. Countries that recently implemented reforms, such as Brazil, Colombia, and Mexico, will need to enhance their internal capacities to effectively track complex money trails. Meanwhile, the delicate nature of prosecution cases involving public officials will require substantial determination and political will.

Prevention better than response

Given recent developments throughout the region and increased scrutiny of business in Latin America by regulators such as the US DOJ and SEC, companies should redouble efforts to enhance their anti-corruption compliance programs. The following four recommendations are worth noting:

» Proper risk assessment: Risks vary from country to country, within different industries or by company depending on the level of government interaction.

Adequate identification of the risks and related exposure is key to tailoring effective procedures and controls.

» Third party due diligence: Companies should look into the details of transactions and their related third parties (e.g., agents, suppliers, joint venture partners) to identify and avoid the risk that third parties could offer bribes on their behalf. The due diligence should provide a good understanding of the third party’s track record, business practices, and reputation. A higher level of due diligence should be conducted on high-risk third parties.

» Due diligence on local investment targets: Investors should undertake in-depth due diligence reviews of the target’s anti-corruption policies and procedures, the target’s culture and leadership stance toward integrity and ethics, and market reputation. A multi-tiered due diligence approach depending on the level of government exposure is recommended.

Training: Many Latin American companies have little to no awareness regarding the requirements of local and international anti-bribery laws. A robust training program should be designed and implemented, and their related activities properly documented. Training should ideally include employees of relevant third parties as well.

While it is too early to predict whether government agencies will aggressively enforce recent anti-corruption laws, companies should certainly expect a higher number of corruption-related prosecutions in Latin America than those observed in the past. Companies that do their homework will be better prepared to prevent incidents, or seek more lenient treatment from the authorities and other stakeholders, should an incident occur.
LATIN AMERICA INFRASTRUCTURE PROJECTS

Dealing with the risks

In the last few years, Latin America has seen a significant uptick in the number of large-scale infrastructure projects, although these rates are still below the 4% to 5% investment that the World Bank estimates is necessary to support expectations of growth in the region.

Notwithstanding these ambitious growth projections, the region has a critical challenge in infrastructure development, caused by a variety of underlying factors. For example, advances in commodity production that occurred in the 1990s have generated a large gap between production systems and increased demand. This disparity is up against an inefficient logistics flow and deficits in energy production—struggling to meet growing industrial activity. Many Latin American governments are aware of the problem and realize that, without significant infrastructure development, their nations will fail to meet internal and external growth expectations. Among others, key areas to address include road transportation networks; hydroelectric and thermoelectric power plants; port modernizations; amplification of railway; increased depth, length, and width of navigable waterways; sporting venues; water sanitation and filtration; petrochemical plants; and oil and gas exploration, production, and refining. The following represent a small sample of the countless projects currently being undertaken in Latin America to help bridge the infrastructure gap:

» Chile is building a water conveyance system called Aquatacama;
» Mexico is constructing the Bicentennial Refinery;
» Brazil plans to build a high-speed rail system;
» Colombia is undertaking a massive transportation project called Highways for Prosperity;
» Argentina is constructing the Truncado transmission power line;
» Uruguay is building the Punta Sayago Liquefied Natural Gas Plant;
» The Dominican Republic is building a corridor to Santo Domingo;
» Ecuador is developing the Dodo Sinclair Hydroelectric plant;
» Panama is developing a major metro line;
» Costa Rica is constructing the Reventazon Hydroelectric project; and,
» Jamaica is expanding its Kingston port.
The increase in infrastructure projects in Latin America will likely bring a broad array of social and economic benefits to the region and support sustainable growth. However, the planning and execution of these projects carry a number of concerns for investors, private companies and government partners operating in the segment. While many organizations have experience working in Latin America, dealing with cultural barriers and geography-specific risks remains a challenge. Armed militant groups, social resistance, crime, legal uncertainty, political interference, logistics, lack of skilled labor and complex tax codes make up a small portion of the litany of risk scenarios that infrastructure investors and developers will have to address.

In order to properly conduct business in high-risk jurisdictions or unfamiliar environments that pose threats to companies or involved counterparties, it is necessary for investors, managers, and related organizations to have structured mechanisms to identify, quantify and mitigate risks. Such a risk-review function should constantly provide data, reports and indices to relevant personnel and help guide the planning and execution of work. In the bidding phase, for example, companies should capture all elements in a proposal to make sure they are technically sound and competitive in price. While developing bids, companies should have a thorough understanding of major competitors, personnel, logistics, equipment suppliers, third-party vendors, raw material costs and technical training as well as regulatory risks, crime rates, the presence of armed groups and other pertinent challenges that could thwart a winning strategy.

In the execution phase of a project, companies need to be sure that its employees and assets are protected; constantly monitor the progress of any construction sites involved in the operation; establish strict internal controls; develop contingency plans; and conduct field intelligence and deploy countermeasures to mitigate risk. Kroll’s experience with projects of this nature have revealed notable issues related to fraud and compliance breaches that can generate large losses for all parties involved. Geography and gaps in 24-hour-a-day monitoring of controls contribute significantly to the perpetration of ethics violations. This issue is highlighted by the survey findings. For example, in Brazil, 74% of companies have been affected by at least one fraud in the past year that has generated an average loss of 1.7% of total annual revenue. In Mexico, the survey demonstrated a year-over-year increase of 19% to 30% of companies reporting an occurrence of asset theft.

Kroll has an extensive history of supporting risk management needs in large infrastructure projects. Our collective work in infrastructure, coupled with our investigative expertise, has provided us with deep insight into the segment. In one recent case, we helped an energy consortium obtain information related to internal factions that aimed to delay the delivery of work. Our fieldwork revealed that a core group of employees was responsible for organizing strikes and delays that would impact compliance with the project’s scheduled timeline. In another assignment with an infrastructure client, Kroll conducted a comprehensive risk assessment for a large-scale project that was located in a hostile geographic environment. The study included reality-based risk scenarios touching on topics such as the safe transportation of employees, materials, and equipment to be used in construction as well as the implementation of internal control measures, access policies, and contingency plans related to managing risk and loss.
CHINA OVERVIEW

This year the data from China-based respondents shows little change in that country’s incidence of fraud. This may, however, mask a growing problem. The proportion of those reporting an increase in fraud exposure at their firms has grown from 69% in the 2012 survey to 80% this time. Moreover, the sense of vulnerability to fraud has grown dramatically: as the chart shows, the proportion of those reporting themselves highly vulnerable to every fraud covered in the survey is much increased, in some cases by an order of magnitude higher.

Prevalence: Companies affected by fraud

<table>
<thead>
<tr>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>67%</td>
<td>65%</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft of physical assets or stock (23%)</td>
<td>22%</td>
</tr>
<tr>
<td>Management conflict of interest (20%)</td>
<td>21%</td>
</tr>
<tr>
<td>Vendor, supplier or procurement fraud (18%)</td>
<td>20%</td>
</tr>
<tr>
<td>Regulatory or compliance breach (15%)</td>
<td>20%</td>
</tr>
<tr>
<td>IP theft (15%)</td>
<td>18%</td>
</tr>
</tbody>
</table>

Increase in Exposure: Companies where exposure to fraud has increased

<table>
<thead>
<tr>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>80%</td>
<td>69%</td>
</tr>
</tbody>
</table>

Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected

<table>
<thead>
<tr>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increased outsourcing and offshoring (44%)</td>
<td>43%</td>
</tr>
<tr>
<td>Entry into new, riskier markets (40%)</td>
<td>33%</td>
</tr>
</tbody>
</table>

Loss: Average percentage of revenue lost to fraud

<table>
<thead>
<tr>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2%</td>
<td>0.8%</td>
</tr>
</tbody>
</table>

Amid this general worry, the survey data also suggests the need for greater attention toward an old problem in China. For many years, foreign companies complained of extensive intellectual property theft in the country. More recently, however, analyses have shifted to speaking of the progress in the area. This may help explain why, in this year’s survey, China-based respondents are only about as likely as those elsewhere to think their companies are at risk of IP theft.

Other data in this year’s survey, though, shows that IP theft remains a significant challenge for companies operating in China. Fifteen percent of respondents report that their companies were affected by this fraud in the last 12 months, the highest level for any country reported on in-depth by the survey. This also represents a substantial rise from the 2012 survey, when only 8% of respondents were affected. In some ways, the danger may even be increasing: 44% report that greater outsourcing is increasing overall fraud exposure – the highest figure for any geography – and 33% say the same for high staff turnover as well as for cost restraint over pay. Unscrupulous suppliers, dismissed staff and disgruntled employees are all common among IP thieves.

On the positive side, 62% of China-based respondents report that their companies plan to invest further in IP protection in the coming year – another survey high. This is money well spent: the battle to safeguard IP in China is far from over.
Chinese entrepreneurship has for centuries been built upon two important attributes: (1) **familism** and (2) **guanxi**, the premise of connections.

**Familism** is the social structure by which the needs of the family are more important than any individual family member. Familism has great influence on business decisions in Chinese society, particularly since many of China’s companies are family-based. Foreign management may find it hard to penetrate this family circle of trust and secure loyalty, making it challenging to enforce corporate decisions.

**Guanxi** refers to the personalized networks of influence these entrepreneurs possess. It is a central idea in Chinese society, which is tightly knit with informal ties and relationships, including relationships with the Chinese government in almost every aspect of social interaction. Guanxi for some companies may mean they are more likely than their competitors to be approved for loans, or they may receive relevant licenses sooner rather than later. These relationships may prove advantageous, but today’s political assets may very well turn out to be tomorrow’s political liabilities. It is essential to understand whether the Chinese partner’s strong relationship with its government counterparts is an institutional alliance based on operational strength and contributions to the local economy, or, more dubiously based on bribery.

Understanding the mind-set of a Chinese entrepreneur

First-generation Chinese entrepreneurs typically come from humble beginnings; they have tasted hardship, but in a growing economy also tasted the sweetness of wealth. As a result, they are highly ambitious and willing to take risks if they sense a maximum pay-out on their investments. This mind-set does not change when there is a transition from a private company to a listed company or from a private company to an international company, which could potentially create corporate governance challenges.

Recognizing the tell-tale signs of fraud

When investing in the “China story,” investors should not be consumed by an entrepreneur’s ambitious pitch until they can corroborate the story. When something sounds too good to be true, investors need to dig deeper. Fraud channelled through third parties is very common in China; the complexity of schemes may be different, but the end result is the same. Investors must confirm the veracity of...
any intermediary contracts and acquisitions the Chinese entrepreneur is pursuing. What may come across as a legitimate revenue-generating acquisition often turns out to be an over-priced purchase of a relative’s business, which simply is a conduit to channel funds back into the entrepreneur’s pocket.

Similarly, sales revenue figures and relationships with distributors should be questioned. For example, a multinational client in the retail sector – who was once impressed by the double-digit sales growth of its China branch – appointed Kroll to investigate the reason behind large accounts receivable that were building up with distributors. Kroll found that the China branch was simply moving goods back and forth from its family-owned distributors. As per the small print in the contracts, the distributor could return all unsold goods with no penalty. The illusion of profitability boosted the company’s share price; however, reality quickly caught up and news of bad debt caused a significant drop in share price and angered investors.

In the West, many companies possess control mechanisms to limit such behavior. These include job rotations, authorization levels, segregation of duties, rendering processes for contracts and internal audits, and more importantly, regulatory requirements such as disclosure of conflicts of interest or external audits. In China, however, these measures may not be enough, especially since junior employees will rarely disagree with senior management, and internal authorization can be easily obtained when the entrepreneur’s family members are the other department heads.

Pre & Post-transaction checks

For foreign investors, conducting extensive and thorough reputation-focused due diligence before entering into a transaction is a priority. This must include a thorough background search on the partners, their business, and track record working with foreign investors. It is important to try and have a clear assessment of the entrepreneur’s true motivation, integrity, and business acumen.

The mistake many investors make is to rest on their laurels after the deal is done. Post-transaction, if possible, it is crucial to conduct an in-depth risk assessment of how the company mitigates or handles instances of fraud, bribery and corruption, money laundering, related-party transactions, and conflicts of interest. Based on the findings, appropriate anti-fraud, anti-corruption measures can be put in place, but given the challenges mentioned above, these will only be of value if managed by a local team put in place by the head office.

Where satisfactory due diligence cannot be conducted before an acquisition, regulators now expect effective post-acquisition due diligence to identify the risks in a relatively short time after the deal. The primary objective of the forensic due diligence is to evaluate the potential future loss in value resulting from inappropriate or unethical business practices of the target. This analysis generally concentrates on specific areas – inventory and supply chain management, consultancy and agency fees, travel and entertainment expenses, political and charitable donations, and cash transactions.

China should not be a place that investors shirk in trepidation; rather, it is a vibrant place where intrepid investors and entrepreneurs can do business for potentially a great reward, but only when done right.

As an investor in China, when was the last time you visited the China presence unannounced or with little pre-warning?

You might be surprised by what you see.

Last year’s consumer goods report card warned that too many companies in this sector were not paying enough attention to vendor or procurement fraud and theft of physical assets. This year’s survey data show the results of such complacency. For the second year in a row, the sector has seen the highest level in the survey of vendor, supplier or procurement fraud. This time, however, the actual incidence is nearly twice as high (20% compared with 10% in 2012). Meanwhile, over the past 12 months theft of physical assets or stock – a traditional bane of the consumer goods industry – affected the companies of 41% of respondents in this sector, the third-highest level of any industry in this survey and again well up on the 2012 survey (26%). Despite these growing problems, consumer goods companies still have the lowest average fraud loss of any sector (0.9% of revenue), although this was more than double the figure in the previous survey. The industry is also moving in the right direction. It has the highest proportion of companies of any sector planning to invest in physical asset security (59%) in the coming 12 months and an above-average 50% of consumer goods companies are looking to invest in partner and vendor screening, up from 33% in the 2012 survey. That said, with 86% of consumer goods respondents saying that their businesses are at least moderately vulnerable to vendor or procurement fraud, plenty of work remains to be done.
India in the past year had a multi-faceted fraud problem, with seven different frauds affecting more than 15% of companies. In particular, over the last 12 months the country had an above average incidence of theft of physical assets (33% of companies were affected compared to 28% for the survey as a whole), corruption (24% compared to 14%), and internal financial fraud (22% compared to 16%). It also had a slightly above average incidence of information theft (24% compared to 22%).

Indian companies understand that they operate in a high-corruption environment: 37% of respondents acknowledge that their firms are highly vulnerable to this fraud, up from 32% last year and well above the survey average of 20%. More broadly, 86% acknowledge at least some vulnerability in this regard.

For other frauds, though, Indian companies seem to be less sensitive to the dangers than their peers elsewhere. Only 12% says that their businesses are highly vulnerable to theft of physical assets, compared to 18% among all companies. The equivalent figures for internal financial fraud are 4% and 13% respectively, and for information theft 14% and 21% respectively—even though in all three cases the actual incidence of fraud is higher in India than globally.

Companies need to avoid accepting that fraud is just a normal part of business. This is especially true given that, according to the survey, insider fraud is particularly rife in India. At those companies that suffered fraud in the last year and where the perpetrator is known, 69% of respondents say that a junior employee played a leading role and 89% said an insider of some sort – a junior, middle management, or senior employee or an agent – did so. Making matters worse, high staff turnover is the second most common factor increasing fraud exposure in India (cited by 29% of respondents). With figures like this, the 51% of companies not planning investment in staff background checks and management controls next year may wish to reconsider.

<table>
<thead>
<tr>
<th>Prevalence: Companies affected by fraud</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft of physical assets or stock (33%)</td>
<td>Theft of physical assets or stock (27%)</td>
<td></td>
</tr>
<tr>
<td>Information theft, loss or attack (24%)</td>
<td>Information theft, loss or attack (23%)</td>
<td></td>
</tr>
<tr>
<td>Corruption and bribery (24%)</td>
<td>Internal financial fraud or theft (22%)</td>
<td></td>
</tr>
<tr>
<td>Internal financial fraud or theft (22%)</td>
<td>Corruption and bribery (20%)</td>
<td></td>
</tr>
<tr>
<td>Vendor, supplier or procurement fraud (20%)</td>
<td>Vendor, supplier or procurement fraud (20%)</td>
<td></td>
</tr>
<tr>
<td>Management conflict of interest (16%)</td>
<td>Regulatory or compliance breach (16%)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft of physical assets or stock (33%)</td>
<td>Theft of physical assets or stock (27%)</td>
<td></td>
</tr>
<tr>
<td>Information theft, loss or attack (24%)</td>
<td>Information theft, loss or attack (23%)</td>
<td></td>
</tr>
<tr>
<td>Corruption and bribery (24%)</td>
<td>Internal financial fraud or theft (22%)</td>
<td></td>
</tr>
<tr>
<td>Internal financial fraud or theft (22%)</td>
<td>Corruption and bribery (20%)</td>
<td></td>
</tr>
<tr>
<td>Vendor, supplier or procurement fraud (20%)</td>
<td>Vendor, supplier or procurement fraud (20%)</td>
<td></td>
</tr>
<tr>
<td>Management conflict of interest (16%)</td>
<td>Regulatory or compliance breach (16%)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Increase in Exposure: Companies where exposure to fraud has increased</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT complexity (33%)</td>
<td>IT complexity (43%)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT complexity (33%)</td>
<td>IT complexity (43%)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Loss: Average percentage of revenue lost to fraud</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.4%</td>
<td>1.2%</td>
<td></td>
</tr>
</tbody>
</table>
However, we are now seeing an increasing number of companies in Asia proactively investigating vendors and employees for suspect relationships and activities. While a stronger emphasis on good corporate governance is driving part of this new focus, we also attribute it to the greater awareness among companies of the losses due to procurement-related fraud coupled with operating in a difficult economic environment that makes it imperative to look for ways to improve the bottom line.

### Challenges to investigating procurement fraud

**Suspicions without proof.** A number of investigations where Kroll has been involved in Asia started as whistle-blower complaints or informal water-cooler discussions about procurement practices that led managers to suspect certain vendors and employees. A major challenge of investigating fraud when there is no evidence against any target is that often managers do not know which vendors and employees to investigate first.

**Accusations without details.** A related challenge is that whistle-blowers rarely come forward to share details such as names of employees who are involved, the scale of the fraud, and how the fraud is perpetrated. Employee loyalty often lies with the local CEOs rather than with the parent company based abroad.

**Internal audit “preparation.”** Internal audits should not be relied on to root out fraud. The scope and schedule of internal audits are often communicated well in advance to minimize business disruptions; however, this increases the risk of “window dressing.”

**Unreliable vendor data.** Poor quality of vendor data is also a key concern when conducting procurement-related investigations in Asia, even when Enterprise Resource Planning (ERP) systems are in place. In one of Kroll’s investigations, the client had entered a large volume of data into SAP when it was first installed in 2006. We determined that the data was poorly entered at the time, with little quality control. This posed a difficult challenge when the client wanted to review the data a few years later to identify suspicious vendors.

**Who is connected, who is not.** In many of our Asia investigations, relatives of politicians, police and bureaucrats are linked to employees or vendors. This is a key issue in several Asian countries where ownership records of companies are not as easily accessible to the public, making it harder to identify conflicts of interest. Companies can face regulatory problems if vendors are linked to government officials or blacklisted companies, rendering the tender process ineffective as applicants may be part of the same parent company.
**Best practices for responding to suspected fraud**

Kroll has helped several companies investigate vendors and employees when procurement fraud is suspected and targets are known. Since there is no “one size fits all” strategy for this region, the most effective approach incorporates both best practices and client-specific considerations. Taking into account a country’s legal framework in which an entity operates, the steps can include:

- **Overt vs. Covert.** There are pros and cons for each option – for example, an overt investigation may lead to the identification of key witnesses but can also result in data loss if a perpetrator catches wind of the investigation and starts destroying critical evidence.
- **Garden Leave.** Consider placing the suspect employee on Garden Leave so that he or she remains on the company’s payroll and is obliged to talk to investigators when summoned.
- **Breach and Clear.** Secure the evidence (i.e., PCs, data and email servers, smartphones and mass storage devices), maintain chain of custody and restrict access to the aforementioned hardware.
- **Secure Evidence.** Secure documents and contents of the target’s desk or office.
- **Block All Access.** Remove access to the server and the premises.
- **Examine Data Files.** Forensically extract data from IT equipment. Also, analyze the data using dedicated text-mining tools. Keywords should be specific to limit false positives.
- **Data Analytics.** Conduct data analytics on suppliers’ master-file, sub-ledger, cash books, expense claims, phone records, general ledger entries, approved contracts and invoices, budget vs. actuals, etc.

### FINANCIAL SERVICES

Although the growth in fraud for financial services this year was consistent with the experience of other sectors, it remains one of the most affected industries in 2012/13. With 75% of companies hit, the sector had the second highest overall incidence of fraud after manufacturing. Moreover, it had the most widespread problems in the survey with internal financial fraud (29%), regulatory or compliance breach (26%) and money laundering (8%). Although it saw a slight decline in the incidence of information theft – to 29%, from 30% in the previous survey – it still had the second highest frequency of this crime in the survey. Meanwhile, the rate at which financial services firms lost money to fraud (1.5% of revenue on average) is both above the median and more than twice the level found in the previous survey. Looking ahead, coping with complexity will be a major challenge for financial services companies. The sector has the highest number of respondents reporting increased fraud exposure from information technology (IT) complexity (47%) and from ever greater complexity of its products (28%). High staff turnover is also cited increasingly as a driver of higher fraud risk (38%) in financial services than in any other sector, making dealing with complicated systems and offerings all the harder.

### ECONOMIST INTELLIGENCE UNIT REPORT CARD

<table>
<thead>
<tr>
<th>Loss: Average percentage of revenue lost to fraud: 1.5%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevalence: Companies affected by fraud: 75%</td>
</tr>
<tr>
<td>Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud: Internal financial fraud or theft (29%) • Information theft, loss or attack (29%) • Regulatory or compliance breach (26%) • Theft of physical assets or stock (23%) • Management conflict of interest (20%) • Vendor, supplier or procurement fraud (18%)</td>
</tr>
<tr>
<td>Increase in Exposure: Companies where exposure to fraud has increased: 79%</td>
</tr>
<tr>
<td>Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected: IT complexity (47%)</td>
</tr>
</tbody>
</table>

### What happens when you suspect fraud but are not sure who are the perpetrators?

In the event of a suspected fraud when targets are unknown, Kroll works to isolate the source of the problem by:

- Analyzing internal data files on vendors and employees in an efficient way to shortlist targets.
- Gathering external evidence from vendors, former employees, competitors and customers about the company’s practices that may constitute fraud.
- Establishing strong, well-organized internal control systems to reduce clients’ vulnerability to procurement fraud.

Visit fraud.kroll.com for web-exclusive content, including more best practices and proven strategies on how to mitigate the risk of procurement fraud in South and Southeast Asia.
This is the first year that the fraud report has focused on Malaysia, and survey respondents reveal a mixed picture.

<table>
<thead>
<tr>
<th>2012-2013</th>
</tr>
</thead>
</table>

**Prevalence:**
Companies affected by fraud

66%

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

- Theft of physical assets or stock (34%)
- Vendor, supplier or procurement fraud (25%)
- Regulatory or compliance breach (16%)

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

69%

**Biggest Drivers of Increased Exposure:**
Most widespread factor leading to greater fraud exposure and percentage of firms affected

- Increased outsourcing and offshoring (41%)

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

0.6%

On one hand, the country had slightly below average incidence of fraud overall, with 66% of businesses suffering from at least one fraud in the last 12 months, compared to 70% globally. Also, for most of the specific frauds covered in the survey the incidence was also below the mean. On the other hand, two types of fraud are worryingly widespread, even by global standards: 34% of companies were affected by theft of physical assets (compared to an overall average of 28%) and Malaysians reported the second highest country rate of vendor or procurement fraud in the world with 25% of companies affected. Only Saudi Arabia’s incidence was higher, at 33%. The danger from vendors shows through in other data as well. For companies that had suffered fraud and where the perpetrators are known, Malaysian respondents are more likely than average to report that vendors were leading parties (38% of cases compared to 32% overall).

Regrettably, companies do not seem to be fully aware of the extent of vendor and procurement fraud in their country with only 9% acknowledging that they are highly vulnerable, compared to 18% globally. Another worry is that the businesses of Malaysian respondents are more likely than companies in almost any other geography to rely on external audits to uncover fraud, and have among the lowest rate of fraud discovered by senior managers. These executives need to become more fully attuned to the issue in order to protect their companies better.
In almost all developing Asian countries, high growth has created the demand for better economic and social infrastructure. These countries have not only expanded tremendously in terms of income and population. They have also experienced rapid urbanization, a growing middle class, and in some countries, the intensifying realization among the political classes – especially in countries where there exists an electoral process – that citizens will judge the performance of their leaders by the economic and social facilities they deliver.
High absolute demand for better infrastructure in South and Southeast Asia occurs at a time when experts claim there is a marked increase in infrastructure investment globally. Conventional wisdom is that economic infrastructure assets are inherently monopolistic and therefore less sensitive to spells of economic weakness. This probably holds true more in developed countries than in developing ones where the risks of political instability, currency depreciation and indeed, the expropriation of an asset could swiftly eradicate the promise of high returns from a monopoly situation. Many foreign investors who were forced to renegotiate contracts or had them canceled in the aftermath of the 1997 Asian crisis would appropriately remind us of this fact. But there are enduring signs of change since that time: there is greater political stability in most Asian countries, currencies are flexible and the public-private partnership model has made wholesale seizure of assets in the infrastructure sector less likely. There are also other factors driving infrastructure investment in Asia:

» Despite inconsistencies in execution, improvements in the business and regulatory environment are reducing barriers to entry. Legislative reforms passed or slated in Indonesia (e.g., amendments to the law on public-private partnerships and land acquisition), Thailand, Philippines and even Myanmar, have coupled with relatively favorable concessions offered to foreign investors by governments looking to attract infrastructure investment.

» The hunger for natural resources; exploration, development, production, transportation and distribution of resources requires good infrastructure. This has been one of the drivers of Chinese infrastructure investment in Southeast Asia (and elsewhere).

» Overcapacity on the part of Japanese and Malaysian companies has forced them to look for new investment opportunities in “near-abroad” markets. These countries, alongside China, have deeper domestic capital markets and therefore able to fund infrastructure investments led by their blue-chip companies. Telecommunication investments in India and recently in Myanmar have also benefited from a similar driver (in these cases, Russian and Middle Eastern petrodollars funded the investments).

» Long-term, open-end infrastructure investment funds have given global investors a new way to bet on emerging markets growth. Allocations are increasing annually. This is not “hot money” that flies the moment that US monetary policy changes. Investors are aware that their capital will be tied up for a long time. Moreover, with the development of regional financial and offshore centers such as Hong Kong and Singapore, funds are finding innovative ways to reduce the impact of foreign exchange risk and to some extent, sovereign risk.

These factors have brought private financing into countries historically unable to fund infrastructure projects.

Risk Mitigation Strategies

There are also negative factors underlying the prospects for infrastructure investment in developing Asia. Based on our conversations with clients, the recent slowdown in China and India, Asia’s two largest growth markets, is not top of their list of concerns – investing in a country’s infrastructure involves betting on long-term growth and the continued demand for services in these countries.

Investors are more concerned about stalled reforms in India and bureaucratic delays in approving projects (Mumbai’s Sea Link famously took 20 years to be approved). Lack of transparency in Indonesia, the prevalence of corruption in Philippines and populist changes to policy all present serious challenges. A political and regulatory risk assessment should be conducted at the outset of infrastructure projects to understand and mitigate these risks. Taking a macro view on probable political scenarios is not enough. It is critical to understand the relative positions of all stakeholders, covering policymakers at the central government level, administrators at the provincial level (or even at the sub-provincial level), local residents, organized labor, and environmental NGOs as well as undisclosed stakeholders such as local businesses with hidden agendas who can alter the outcome of a project.

For example, in 2012, spurred by legislative reform, a Japanese-led consortium won the bid to build a new power plant in Central Java that would provide electricity for 8 million people. However, this year certain landowners refused to sell a portion of land accounting for 20% of the planned construction site. If the dispute is not resolved in time, the consortium faces losing the concession. An in-depth market entry assessment conducted at the outset of the investment cycle may have identified this risk.

It is also important to conduct benchmarking of competitors at the tender stage. This exercise will not only inform a more effective bid, but could also mitigate the risk of competitors seeking annulment of a concession after the tender is closed.

In the construction phase of the investment cycle, supply chain issues always surface. This is not just a matter of performance risk. Fraudulent collusion between suppliers and local managers (or managers of JV partners) can give rise to large financial losses and cause delays in the project, heightening completion risk. If bribery and corruption issues emerge, the project can be embroiled in debilitating controversy and serious legal problems, locally and internationally. Over and above the initial due diligence of subcontractors and partners, Kroll is frequently asked to conduct regular fraud reviews to mitigate the risk of corruption and theft as well as contract audits to reduce the risk of overpaying. Such assignments require the deployment of investigators with experience working in the locality supported by forensic accountants and data analytics experts.

Companies in the infrastructure sector are accustomed to assessing market conditions before making massive upfront investments. They may have a history of studiously considering political and regulatory risk before stepping into an environment of multiple competing interests, where pricing policies or tax regimes can suddenly change at any point in the long investment cycle. All these risks can be managed, especially against the backdrop of favorable politico-economic trends. But infrastructure is ultimately an investment in an operating business, and the realities of operating in South and Southeast Asian countries may present risks with which many companies are unfamiliar.

Omer Eginsoy is a Senior Managing Director for Kroll based in Singapore. Omer has extensive experience in conducting corporate and regulatory investigations and in providing dispute advisory and litigation support services to clients. His areas of expertise include emerging markets, special situation investments, complex multi-jurisdictional commercial disputes and hostile takeovers. He also has a long track record of advising high net worth individuals on reputational and regulatory issues and in leading confidential reputation audit assignments for emerging market business owners.

Makoto Suhara is a Managing Director based in Tokyo, specializing in business intelligence, fraud investigation, corporate governance and risk consulting services for multi national corporations and government agencies. Makoto has helped clients respond and mitigate risks in the areas of financial fraud, legal dispute, regulatory and compliance, and computer security.
Europe, Middle East and Africa

Regional Analysis

The perceived extent of fraud on the continent depends on perspective. It is not widespread compared to certain developing regions. From a global perspective, though, Europe is not a low fraud location either. Overall, fraudsters hit 73% of businesses at least once during the last year, which is slightly above the survey average (70%). Moreover, for all but one individual fraud covered in the survey, the European incidence was within 2.5% of the global figure. The sole exception was information theft, which was slightly more common on the continent (25%) than overall (22%).

The survey figures also show fraud becoming more prevalent in Europe during the last year, as was the case in much of the rest of the world. Every fraud covered in the survey was more common in Europe this year than in the 2012 survey. In particular, the incidence of theft of physical assets went from 23% to 28%; information theft from 18% to 25%; management conflict of interest from 13% to 21%; and internal financial fraud from 12% to 17%.

Similarly, fraud losses rose from just 0.8% of revenues to 1.2%. The growth in fraud exposure indicates that these numbers may increase further: 77% report an increased overall fraud risk this year, up from 56% in the 2012 survey.

Despite their growing fraud problem, European companies are less likely than their peers elsewhere to be taking action against it. For all but two of the anti-fraud strategies covered in the survey, Europeans are the least likely of those in any region to have planned investment in the next year. For the two exceptions – financial controls and management controls – they are the second least likely. Greater attention will be needed if Europe wants to reverse the recent increase in fraud.

Europe has a growing fraud problem, but the survey data suggests too many companies exhibit a dangerous complacency.

<table>
<thead>
<tr>
<th>Prevalence: Companies affected by fraud</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>73%</td>
<td>63%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft of physical assets or stock (28%)</td>
</tr>
<tr>
<td>Information theft, loss or attack (25%)</td>
</tr>
<tr>
<td>Management conflict of interest (21%)</td>
</tr>
<tr>
<td>Internal financial fraud (17%)</td>
</tr>
<tr>
<td>Vendor, supplier or procurement fraud (17%)</td>
</tr>
<tr>
<td>Theft of physical assets or stock (23%)</td>
</tr>
<tr>
<td>Information theft, loss or attack (18%)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Increase in Exposure: Companies where exposure to fraud has increased</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>77%</td>
<td>56%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT complexity (37%)</td>
<td>IT complexity (27%)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Loss: Average percentage of revenue lost to fraud</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2%</td>
<td>0.8%</td>
<td></td>
</tr>
</tbody>
</table>
Cyber criminals love advisors, but not because they guide them through legal issues or help them hide their ill-gotten gains. Rather, of all a cyber criminal’s potential targets, advisors present the best value for money.

The psychology of a cyber criminal

Cyber-based crime has different motivators, different methodologies, and different targets. While the media likes to use the word cybercrime for every computer-based attack, the term is really about profit-motivated attacks. Cyber criminals are financially motivated fraudsters who use the Internet to access data and facilitate their main objective: to make a profit. Although cyber criminals may view themselves as smart business people who “work smarter, not harder,” the reality is that the techniques cyber criminals typically employ are lazy.

As personal cyber security systems have become more robust and user-friendly, it has become harder for financially motivated hackers (FMHs) to collect the data they need. Targeting only one individual at a time, breaking through each unique security system, and then committing a fraud on that one target with no guarantee of success is not a good return on investment or time. Therefore, FMHs like volumes of data from which they can attempt mass fraud schemes, tweaking each attempt to ensure the highest level of success. As well as holding large volumes of data, the ideal target will usually have three main attributes: (1) limited cyber security; (2) full access to the system or network on which they are based; and (3) IT support staff who are just that, “support” rather than security focused.

Professional services firms such as lawyers, accountants, consultants and wealth managers are an attractive target as they typically hold volumes of valuable data which are often stored in an organized manner with little protection.

Professional services: the perfect target

By gaining access to a lawyer’s email accounts, not only can hackers read about upcoming transactions or litigation, they can also impersonate a victim’s lawyer or gain enough personal data to effect wire transfers, property sell-offs, or any other manipulation available to them. The same can be said about the accounts of wealth managers or accountants.
Such attacks are not sophisticated hacks. Most involve a simple password collection made when the adviser logs on at a free Wi-Fi spot or clicks on a link in a spear-phishing email that requires or automates a software download before viewing a file or a video that has gone viral.

Spear-phishing emails are tailor-made for a specific person or professional group with the focus on getting that person or group to click a link and install hidden malware. Professional services advisors are profiled by the attackers utilizing social media, standard media, client inquiries and public records to determine their likelihood of having access to the data required by the cyber criminals.

That profile is used to tweak the attack and then launch it. Ever wonder why you get so much spam or why you have so many new Facebook, LinkedIn, or Twitter followers? Even friendly emails with sugar-coated offers likely be someone willing to pay for it.

### Complacent thinking

Cyber criminals rely on complacent thinking. Many professionals believe that if their email was compromised, they would notice unusual traffic. Unfortunately, once a hacker has access to a victim’s email account, he or she can set up filters to forward certain mail messages away from the hacked inbox to folders or even to reply and then delete before the target sees them.

Even in rare cases where the fraud is discovered and halted in time, cyber criminals will have already stolen information and can use it against victims in a future attack or to make a profit. The financial value of confidential data cannot be underestimated. If it is sensitive, there will likely be someone willing to pay for it.

### Protecting yourself from working for a hacker

The severity of the risk is brought home when two key questions are considered:

- If you discover a compromise on your system, do you have any way of knowing what was viewed, modified, or taken?
- What would be the impact to your business if it became public that client data was stolen and potentially misused?

In the past year, Kroll has been engaged on more than 25 such matters for large professional services firms. The message behind this trend is clear: why attack on a one–on–one basis when a single targeted attack can get you 1,000 victims or more?

The damage to firms in the professional services sector is equally multiplied. In a sector that relies on trust and belief that client information will be protected, the effects can reverberate for years.

The assumption is often made that there is nothing of value that cyber criminals could want, therefore it is not a concern. But the truth is that cyber criminals do not discriminate; they want a lot of data, some of which may seem irrelevant to others. A personal credit card number is just a small piece.

Businesses need to understand what data they hold, why it is important or attractive to cyber criminals, how it is protected, and who has access to it. A proactive understanding of the threats leads to proactive mitigation.

The next time you are “inconveniently” forced to change your password due to some internal policy understand that this, as well as other requirements, could be the difference between money in your hands and money in the cyber criminals’ hands. It could be the difference between working for your client and working for a hacker.
Organized crime infiltration in the supply chain

By Marianna Vintiadis

Obviously some of the proceeds of organized crime groups come from illegal activities that are both well-known and readily identifiable, such as drugs, prostitution, and racketeering. An increasingly important part, however, emerges from more discreet activities such as infiltrating the supply chain of legitimate businesses.

Legambiente, the Italian League for the Environment, set up an Observatory on environmental crimes in Italy in 1994. Each year, the Observatory publishes a report on crimes affecting the environment covering a number of areas, such as construction, waste, arson, and archaeological crime. According to the 2013 Ecomafia report, the turnover of environment-related crimes for Italian organized crime groups has reached €16.7 billion and the Italian local administrations dissolved by Presidential Decree due to mafia infiltration has risen from 6 to 25.

These crimes do not affect Italy alone. The dumping of toxic waste in Somalia by Italian organized crime gangs has had an impact on the local population, international troops and, following the 2004 tsunami, on many distant shores. Aside from the obvious and disastrous health hazard caused by the dumping, this “trade” is widely alleged to be connected to the piracy of recent years: organized crime groups supply Somali warlords with arms in return for permission to dump waste.

If toxic waste dumping affects a small section of the business community, other activities have broader ramifications. The Italian authorities seized assets worth €1.3 billion...
from Sicilian businessman Vito Nicastrì last April. Nicastrì, dubbed by the Italian media as “Lord of the Wind,” is alleged to be a mafia frontman in the renewable energy sector.

Italy’s favorable subsidy regime led many investors to seek opportunities in Italian renewable energies over the past decade. Companies, individual investors, and many private equity funds who dealt with Nicastrì are now fighting seizures and the inevitable reputational damage that has ensued. Many of those affected are foreign investors who failed to conduct appropriate due diligence.

Construction is another area traditionally associated with the mob. Fear of infiltration in the reconstruction efforts following the earthquakes that hit the region of Emilia Romagna last year has led the authorities to create a “white list” of construction companies. Although adherence to the list is voluntary, only white list companies can bid for public contracts in the region. The aim here is not only to protect the region from infiltration, but also to protect workers by ensuring that proper contracts and health and safety regulations are adhered to.

Organized crime infiltration in the construction industry is not only an Italian problem. It is well-known that major efforts have been undertaken in several other countries including the United States to curb the power of the “families.” Evidence emerging from Quebec’s Charbonneau commission of inquiry on the awarding and management of public contracts in the construction industry is just one recent example suggesting that organized crime infiltration is still alive and well in North America. The public inquiry is still ongoing, but many allegations about illegal political financing, bid-rigging, collusion, and mafia ties in Quebec’s construction industry have already come to light.

Transport is another major area where infiltration occurs as the freight business offers synergies with drug trafficking and other forms of illegal cross-border trade. Dutch freight and delivery group TNT Express fell victim to the Calabrian ’ndrangheta and Milan magistrates had to take temporary control of a number of its branches in Lombardy in 2011. So, even large and reputable multinationals are not beyond infiltration.

Energy, construction, and transport are important examples of areas in which company supply chains can become polluted. Any company may need to build a new plant, repair its buildings, transport its goods, or decide to diversify its portfolio into renewables. The threat is increasing as clans diversify into the legal economies of developed countries. And the perils for businesses and investors are also on the rise as health and safety, anti-bribery and corruption legislation may implicate not only the supplier but the company awarding the contract as well.

But a solution is available: applying appropriate due diligence checks can go a long way to mitigate the risk. Supply chains can involve thousands of third parties, so a methodological approach should be applied to segment risk and prioritize red flag situations which may require deeper analysis. Third party risk assessment tools use algorithms to quickly process risk profiles, enabling companies to identify which relationships might pose the greatest threat to their organization. Armed with this information, companies are better able to prioritize future due diligence efforts, for example checking links to known criminals. Organized crime generally moves in families, and many organizations, from police forces to observatories and charities, will publicize the criminals’ names and names of known affiliates and sectors of operation.

Reconstructing family ties is a key exercise in attempting to determine links with organized crime. Legambiente identified 34,120 crimes in its last Ecomafia report, these were down to 302 clans – a significant but much more manageable number of repeat offenders to look out for.

**TRAVEL, LEISURE & TRANSPORTATION**

The fraud picture this year for the travel, leisure and transportation industry is relatively positive when compared with the other sectors in this survey. It has the lowest overall incidence of fraud (63%), as well as the smallest figures for management conflict of interest (14%) and market collusion (4%). Moreover, the sector has the second lowest average percentage of revenue lost to fraud (1%). Nevertheless, notable weaknesses exist. The industry has the highest incidence of misappropriation of company funds (14%) and the second highest rate of regulatory or compliance breach (23%). Respondents from this sector recognize the danger: for both of these types of fraud they are more likely to rate their firms as at least moderately vulnerable than those surveyed from any other industry. Meanwhile, cost-reduction strategies are also having a negative effect: 35% say that increased outsourcing has raised the risk of fraud – the second-highest figure for any industry in this survey – and 29% said the same of pay restraint – the highest sectoral figure. Finally, travel and entertainment businesses were not exempt from the general rise in fraud affecting most other industries. Overall, although the good news is welcome, the industry should focus on reducing its vulnerabilities, lest they grow into bigger problems.

**ECONOMIST INTELLIGENCE UNIT REPORT CARD**

<table>
<thead>
<tr>
<th>Fraud Factor</th>
<th>0%</th>
<th>10%</th>
<th>20%</th>
<th>30%</th>
<th>40%</th>
<th>50%</th>
<th>60%</th>
<th>70%</th>
<th>80%</th>
<th>90%</th>
<th>100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corruption and bribery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Theft of physical assets or stock</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Money laundering</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory or compliance breach</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal financial fraud or theft</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Misappropriation of company funds</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information theft, loss or attack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP theft, piracy or counterfeiting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendor, supplier or procurement fraud</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management conflict of interest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Market collusion</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

**Prevalence:** Companies affected by fraud: 63%

**Areas of Frequent Loss:** Percentage of firms reporting loss to this type of fraud:
- Theft of physical assets or stock (23%)
- Regulatory or compliance breach (23%)
- Information theft, loss or attack (17%)

**Increase in Exposure:** Companies where exposure to fraud has increased: 77%

**Biggest Drivers of Increased Exposure:** Most widespread factor leading to greater fraud exposure and percentage of firms affected: increased outsourcing and offshoring (35%)
Africa retains its position as the region with the largest fraud problem.

Sub-Saharan Africa retains the unenviable distinction of having the most widespread fraud problem of any region in the survey. Not only was its overall incidence the biggest in the survey (77% of respondents say that their companies were hit), it had the highest regional figures for theft of physical assets (47%), corruption (30%), regulatory or compliance breach (22%), internal financial fraud (27%) and misappropriation of company funds (17%). As a result, it also has the highest regional level of fraud loss (2.4% of revenues).

Although the overall incidence has not changed since last year, those of individual frauds have shifted markedly. A few are less widespread – information theft noticeably so (19% down from 34%) – but most of the news is bad. Theft of physical assets hit 47% of companies (compared to 32% in the previous survey), vendor or procurement fraud 23% (up from 9%), and regulatory or compliance fraud 22% (compared to 14%). Rather than progress taking place in any given area, this suggests that the fraud situation is unstable, with fraudsters varying their strategies over time.

Meanwhile corruption remains a deeply rooted problem in Africa. The number of companies affected by it this year rose to 30% from 20% in the last survey. More alarming, 48% of African respondents say that their firms are highly vulnerable to this crime. It is therefore not surprising, where a fraud has taken place in the last year and the perpetrator is known, that 33% of respondents say government officials played a leading role in the crime – another highest regional figure.

African companies do not need to look beyond their doors, however, for possible fraudsters. For companies that have suffered fraud and know the perpetrator, the continent has the greatest level of involvement by senior or middle management employees (41%) and by junior employees (51%).

<table>
<thead>
<tr>
<th>Area of Frequent Loss</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft of physical assets or stock (47%)</td>
<td>Information theft, loss or attack (34%)</td>
<td></td>
</tr>
<tr>
<td>Corruption and bribery (30%)</td>
<td>Theft of physical assets or stock (32%)</td>
<td></td>
</tr>
<tr>
<td>Internal financial fraud or theft (27%)</td>
<td>Internal financial fraud or theft (30%)</td>
<td></td>
</tr>
<tr>
<td>Vendor, supplier or procurement fraud (23%)</td>
<td>Management conflict of interest (25%)</td>
<td></td>
</tr>
<tr>
<td>Regulatory or compliance breach (22%)</td>
<td>Corruption and bribery (20%)</td>
<td></td>
</tr>
<tr>
<td>Management conflict of interest (22%)</td>
<td>Information theft, loss or attack (19%)</td>
<td></td>
</tr>
<tr>
<td>Information theft, loss or attack (19%)</td>
<td>Misappropriation of company funds (17%)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Increase in Exposure</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>86%</td>
<td>73%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Biggest Drivers of Increased Exposure</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT complexity (48%)</td>
<td>IT complexity (50%)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Loss</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4%</td>
<td>1.6%</td>
<td></td>
</tr>
</tbody>
</table>
Investment in African infrastructure

AN OPPORTUNITY FOR THE PRIVATE SECTOR

As the bleak outlook for domestic growth drives many Western companies to consider expanding overseas into unfamiliar markets, sub-Saharan Africa is an increasingly attractive prospect.

By Alexander Booth

Economic performance over the past decade has outstripped any previous period, and current forecasts are that the regional African market will grow at about 5.5% this year. Armed conflict is significantly reduced, providing the stability required for economic growth and development. Many state-owned enterprises have been privatized, and legal and regulatory systems are being strengthened. Inflation is being brought under control, and foreign debt and budget deficits are being reduced. Across the continent, African economies have opened up to international trade.

But while in recent years the African investment narrative has been dominated by success in the natural resources and telecoms sectors, today it is the infrastructure sector – which has been estimated to require investments by non-government entities of US$100 billion each year until 2020 – that is most likely to rouse interest and generate returns.

Current infrastructure provision varies among all African countries, but all (except South Africa) fall short of the global average. The deficits are far from uniform, however. In Nigeria, for example, Internet usage is at 90% of global average, while Mozambique is at a mere 12%, a disparity partly explained by the different levels of access to undersea fibre optic cables on the east/west coasts. In contrast, Gabon has a comparatively high per capita spending on health compared to Nigeria, and indeed to China and India, explained partly by its high oil revenues and small population.

By far the greatest infrastructure challenge facing Africa is reliable power provision. Only 16% of the sub-Saharan African population has access to electricity (compared to 50% in Asia and 80% in Latin America). Moreover, some 30 African countries face regular power shortages, forcing many to pay high premiums for emergency power. In some countries, this is becoming a political issue. It was a recurring theme in the 2011 elections in Nigeria, and for many Nigerians it will be an issue as they consider whether to re-elect President Goodluck Jonathan in 2015.

Perhaps the second biggest infrastructure challenge is inadequate transport links. Defunct or poorly maintained rail networks put an added burden on roads, which are frequently starved of investment, in poor condition, and organized more in accordance
with the historical imperatives of colonial rule than with today’s regional realities. As a result, transport costs are the highest in the world – equivalent to 13% of the cost of trade in Africa, compared to 6% worldwide – with an accordingly negative effect on competitiveness. And the transport shortfall is not merely an academic debate: it has a very real impact. In February this year, when global mining major Rio Tinto was forced to book a US$14 billion impairment and chief executive Tom Albanese chose to step down, a key contributing factor was Rio’s losing struggle with rail infrastructure in Mozambique. Rio had acquired substantial coal assets in the country but could find no viable export route through which to monetize the reserves.

Beyond power and transport, other sectors ripe for attention include healthcare, Internet provision, and water/sanitation. The combination of rapidly growing African economies, the commodities boom, increased appetite for private sector participation, a variety of financing models, and a wide range of opportunities across the infrastructure landscape make the investment thesis in this sector particularly compelling.

Preparation is critical

Businesses moving into Africa, however, encounter a set of risks they may not be familiar with from previous transactions. The risk is not confined to the failure of the specific deal in question; the wider fallout may also extend to lasting damage to the investor’s reputation at home. Reasons for failure are many but some – exposure to fraud and corruption, undisclosed interests, personality clashes, and links to organized crime – can be uncovered before committing to a transaction.

The political environment, too, requires close attention and specialist assessment. African democratization is very real, with the one-party state increasingly the exception rather than the rule. Most African countries have transitioned, or are transitioning, toward some form of participatory democracy. But this has not necessarily led to a more stable investment environment. As Côte d’Ivoire, Kenya, and others have shown, election results are frequently contested, overturned, or accompanied by outbreaks of violence. Governments can be fragile and brief in duration. Institutions can matter less than individuals.

So, while there is a potential tremendous upside to doing business in Africa, investors must not be distracted from the challenges and restraints. Investments in infrastructure are particularly vulnerable because of the scale and longevity of the financial commitments, and the need to interface closely with government. Moreover, many hidden risks are not always identified by traditional legal and financial due diligence. Kroll’s recent work in Africa, including infrastructure-related projects, has seen many categories of fraud ranging from regulatory and compliance breaches, through to management conflicts of interest and vendor, supplier, or procurement fraud. Dedicated profiling should be carried out on the commercial track record and industry reputation of potential partners and acquisition targets in order to determine whether a particular relationship presents inherent or specific vulnerabilities. Additionally, it is only by fully understanding where power lies, how it is exercised, and who might bring influence to bear on a partner or acquisition target that investors can accurately gauge this risk, increase the chance of controlling it, and create a stronger framework for realizing a return on their investment.

After having some of the lowest fraud figures in the 2012 survey, in this year’s report the healthcare, pharmaceutical and biosciences sector has the third-highest overall sectoral incidence of fraud (74%), along with one of the largest proportions of respondents seeing an increase in fraud exposure (85%). Rather than any single type of fraud being particularly large for this industry, the problem seems to be that, as the 2012 healthcare report card noted, it is not taking active enough steps to deal with the fraud challenges arising from the business model change which is so common in the industry. Faced with the need to react to healthcare reform in many countries, as well as— for pharmaceutical companies—the need to improve success from research and development spending, the field is seeing dramatic growth in outsourcing and partnerships as well as headcount reduction. The survey shows that these trends are having an effect. For companies hit by fraud where the perpetrator was known, 23% report a joint venture partner was involved (the highest figure in the survey) and 30% an agent or intermediary (the third-highest). Moreover, 43% report that greater outsourcing and offshoring has raised their exposure to fraud (another survey high) and 29% attribute this to increased use of joint ventures and partnerships (the second-highest industry figure). Meanwhile, high staff turnover, in part owing to headcount reduction in the industry, is also heightening risk at 37% of healthcare companies. In response, however, just 45% of healthcare and pharmaceutical firms are planning to invest in due diligence and 43% in staff background checks—both figures are only slightly over the survey average. If business model change is not accompanied by revised fraud defense, the incidence of fraud in the sector is likely to rise further.
Russia had a substantial fraud problem in the last year, with 76% of respondents reporting that their companies have been hit by at least one fraud, one of the highest figures in the survey among countries with sufficient respondents to calculate a figure. Russian firms also report losing on average 1.9% of revenues to fraud, well above the 1.4% average. Especially large problems facing the country are corruption and information theft: it has the highest reported incidence of any country for the former — 32%, more than twice the survey average of 14% — and the second highest incidence of information theft (29%).

<table>
<thead>
<tr>
<th>Prevalence: Companies affected by fraud</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>76%</td>
<td>61%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corruption and bribery (32%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information theft, loss or attack (29%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management conflict of interest (24%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal financial fraud (18%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Theft of physical assets or stock (15%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Theft of physical assets or stock (26%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information theft, loss or attack (26%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Corruption and bribery (16%)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Increase in Exposure: Companies where exposure to fraud has increased</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>74%</td>
<td>52%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT complexity (35%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entry into new, riskier markets (23%)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Loss: Average percentage of revenue lost to fraud</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.9%</td>
<td></td>
<td>0.4%</td>
</tr>
</tbody>
</table>

Just as worrying as the high incidence of fraud are indications that even where companies recognize the risk of fraud, the steps taken are not always the most robust. For example, 91% of those surveyed admit that their firms are at least moderately vulnerable to information theft. Accordingly, 74% of companies plan to invest in information security in the next 12 months, the second highest country figure in the survey. Digging deeper, though, the emphasis seems to be narrowly focused: 71% plan to invest in new security software, but only 59% will invest in training IT employees (compared to a survey average 60%) and just 32% in training employees across the company (survey average 57%). Russian companies are also less likely to be prepared when information theft hits: only 41% have an incident security plan updated in the last 12 months (survey average 53%) and just 32% have tested it in the last six months (survey average 48%). This may reflect a wider lack of effort against fraud: an astonishing 0% of companies report fraud being uncovered via an external audit during the past year. Defenses need to be improved if Russian companies are to see a drop in fraud levels.
Respondents last year reported that the Gulf States were one of the lowest fraud regions globally. This time around, the results are substantially different. The overall incidence of fraud — 72% of respondents report their company being hit once in the last 12 months — was slightly above average, but the increase from the 2012 figure of 49% was more than twice as great as that experienced in the rest of the world.

Moreover, the survey finds that the Gulf States currently have the highest regional incidence of information theft (35%), vendor or procurement fraud (30%), market collusion (28%), and management conflict of interest (24%). The average financial cost of fraud — 1.6% of company revenues — is also above the survey mean.

Accordingly, respondents are worried: 89% say fraud exposure has increased in the past year, up from 54% last year. Moreover, over 20% of respondents believe that their firms are highly vulnerable to every fraud covered in the survey except money laundering. In five cases the region has the most companies reporting this degree of vulnerability: information theft (39%), internal financial fraud (26%), misappropriation of company funds (24%), market collusion (24%), and money laundering (22%).

These concerns are leading a higher proportion of Gulf companies to invest in information security and financial controls than the average of their peers elsewhere. They may, however, wish to consider a wider range of investments. Where a fraud has taken place and the perpetrator is known, for example, those in the Gulf are the most likely of any respondents to report that vendors (46%) or customers (46%) were involved. Nevertheless, only 46% of all regional companies plan to invest in client or vendor due diligence in the coming year, not far above the survey average (42%). Similarly, only 2% of Gulf companies report that a fraud came to light via a whistle-blower during the last year, compared to 22% globally. This suggests a fruitful area to improve fraud defenses, but only 41% of Gulf companies will be investing in staff training and whistle-blower hotlines in the next year, less than the global mean of 43%.
## Summary of sector fraud profiles

<table>
<thead>
<tr>
<th>Sector</th>
<th>Fraud Damage*</th>
<th>Response **</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natural Resources</td>
<td>Medium</td>
<td>High</td>
<td>The sector saw the highest incidence of corruption and bribery of any industry. Although corruption is a well-known issue, natural resources companies also need to pay more attention to vendor or procurement fraud which occurs within the sector at an above average rate. A below average number of sector respondents, though, believe that their companies are even moderately vulnerable to this fraud and investment in due diligence is only about average.</td>
</tr>
<tr>
<td>Consumer Goods</td>
<td>Low</td>
<td>High</td>
<td>The sector had the highest level of vendor, supplier or procurement fraud this year, which also nearly doubled since the 2012 survey. Meanwhile theft of physical assets or stock was at the third highest level of any industry and again well up on last year. On the other hand, the consumer goods companies have the lowest average fraud loss of any sector and large numbers are investing in physical asset security and partner and vendor screening.</td>
</tr>
<tr>
<td>Healthcare, Pharmaceuticals and Biotechnology</td>
<td>High</td>
<td>High</td>
<td>The sector has the third highest overall sectoral incidence of fraud this year, along with one of the largest proportion of respondents seeing an increase in fraud exposure. Common business model changes within the industry are raising fraud risks, including greater use of outsourcing and joint ventures. The industry needs to adjust its anti-fraud strategies accordingly.</td>
</tr>
<tr>
<td>Travel, Leisure and Transportation</td>
<td>Low</td>
<td>Medium</td>
<td>The industry has the lowest overall incidence of fraud as well as the smallest figures for management conflict of interest and market collusion. Weaknesses, though, include the highest incidence of misappropriation of company funds and the second highest of regulatory or compliance breach. Meanwhile, cost reduction strategies, such as outsourcing and pay restraint, are adding to fraud exposure.</td>
</tr>
<tr>
<td>Financial Services</td>
<td>High</td>
<td>Medium</td>
<td>The sector remains among the most affected by fraud this year, with three-quarters of companies hit at least once. It had the most widespread problems in the survey with internal financial fraud, regulatory or compliance breach, and money laundering. Coping with complexity will be a major challenge: the sector has the highest number of respondents reporting increased fraud exposure from IT complexity and from the ever greater complexity of its products.</td>
</tr>
<tr>
<td>Construction</td>
<td>Medium</td>
<td>Medium</td>
<td>The industry had the highest incidence of management conflict of interest, the second highest rate of corruption and market collusion, and the third highest of vendor or procurement fraud. Firms are having difficulty grappling with globalization and the greater use of partners and joint ventures. Entry into new, riskier markets is the biggest driver of increased fraud exposure, and the sector saw the highest proportion of respondents saying that increased collaboration between firms was also raising fraud risk higher.</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>High</td>
<td>Low</td>
<td>The industry, despite some decline in fraud since the last survey, has the highest overall incidence and the second highest rate of financial loss. It is also prone to insiders seeking dishonest gain, with over half of all companies suffering a fraud at the hands of an employee or agent in the last year. Sector companies, however, are not defending themselves aggressively with the number planning investment in a range of anti-fraud strategies in the next year either average or below average.</td>
</tr>
<tr>
<td>Retail, Wholesale and Distribution</td>
<td>Medium</td>
<td>Low</td>
<td>The sector had a substantial theft problem over the last year, with the number of companies with physical assets taken almost doubling. A worrying number of companies, though, may be accepting this as a fact of life: only around half of those companies which are highly vulnerable to theft are investing in new physical security measures. Things could get worse as the industry had the highest number indicating that their exposure to fraud overall rose in the last year.</td>
</tr>
<tr>
<td>Technology, Media and Telecommunications</td>
<td>Medium</td>
<td>Low</td>
<td>This industry combined the lowest overall incidence of fraud with the highest average loss to fraud as a proportion of revenue. Having the highest level of information theft, loss or attack of any sector helped drive up costs. Although the industry is investing in technological defenses, it should consider greater spending on physical asset security: theft of physical devices containing data was the most common mode of information attack this year.</td>
</tr>
<tr>
<td>Professional Services</td>
<td>Low</td>
<td>Low</td>
<td>The sector saw a decrease in overall fraud levels and had the lowest incidence of theft of physical assets, vendor or procurement fraud, and internal financial fraud. Complacency, however, is a danger. Sector companies are noticeably less likely to invest in many common anti-fraud strategies even though their average financial loss to fraud was the same as that of other industries.</td>
</tr>
</tbody>
</table>

* Frequency of fraud and level of financial loss  
** Planned investment in anti-fraud strategies
Contact Kroll

For information about any of Kroll’s services, please contact a representative in one of our offices below or visit www.kroll.com

CORPORATE HEADQUARTERS
600 Third Avenue
New York, NY 10016

GLOBAL REPRESENTATIVES

North America | Latin America | Europe, Middle East & Africa | Asia
--- | --- | --- | ---
Robert Brenner
New York
1 212 833 3334
rbrenner@kroll.com
Recaredo Romero
Bogotá
57 1 742 5556
rromero@kroll.com
Tom Everett-Heath
London
44 207 029 5067
teverettheath@kroll.com
Tadashi Kageyama
Hong Kong
852 2884 7788
tkageyama@kroll.com

North America
Bob Viteretti
New York
1 212 833 3211
rviteretti@kroll.com
David Holley
Boston
1 617 210 7466
dholley@kroll.com
Melvin Glapion
Los Angeles
213 443 1142
mglapion@kroll.com
Bill Nugent
Philadelphia
1 215 568 2440
bnugent@kroll.com
Betsy Blumenthal
San Francisco
1 415 743 4800
bblument@kroll.com
Simone Maini
Washington D.C.
1 571 521 6192
smaini@kroll.com

Latin America
Ray Blackwell
Bastrop
1 512 321 4421
rblackwell@kroll.com
Jeff Cramer
Chicago
1 312 345 2750
jcramer@kroll.com
Brian Lapidus
Nashville
1 866 419 2052
blapidus@kroll.com
James McWeeney
Reston
1 703 860 0190
jmweeney@kroll.com
Peter McFarlane
Toronto
1 416 813 4401
pmcfarlane@kroll.com

Latin America
Dan Karson
Miami
1 305 789 7100
dkaron@kroll.com
Recaredo Romero
Bogotá
57 1 742 5556
rromero@kroll.com
Matias Nahon
Buenos Aires
54 11 4706 6000
mnahon@kroll.com
Brian Weihns
Mexico City
52 55 5279 7250
bweihns@kroll.com
Snezana Petreska
Sao Paulo
55 11 3897 0900
spetreska@kroll.com

Asia
Colum Bancroft
Hong Kong
852 2884 7788
cbancroft@kroll.com
Violet Ho
Beijing
86 10 5964 7600
vh@kroll.com
Reshma Khurana
Mumbai
91 22 6724 0500
rkhurana@kroll.com
Violet Ho
Shanghai
86 21 6156 1700
vh@kroll.com
Penelope Lepeudry
Singapore
65 6645 4520
plepeudry@kroll.com
Makoto Suhara
Tokyo
81 3 3509 7100
msuhara@kroll.com

Europe, Middle East & Africa
Zoe Newman
London
44 207 029 5154
znewman@kroll.com
Yaser Dajani
Dubai
971 4 449 6714
ydajani@kroll.com
Javier Cortés
Madrid
34 91 310 6720
jcortes@kroll.com
Mariana Vintiadis
Milan
39 02 8699 8088
mvintiadis@kroll.com
Alex Volcic
Moscow
7 495 969 2898
avolcic@kroll.com
Bechir Mana
Paris
33 1 42 67 81 46
bmana@kroll.com

Scan the code to read more web-exclusive content or visit fraud.kroll.com
© 2013