BENCHMARKER
Legal Week
Legal Week Intelligence
FRAUD AND CORRUPTION
September 2013

Cities of gold?

FRAUD AND CORRUPTION IN EMERGING MARKETS: A SURVIVAL GUIDE

IN ASSOCIATION WITH

Kroll®

Emerging markets are enticing for any firm looking to expand, but they also present particular difficulties for the unprepared. **Mark Smulian** explains why a little local knowledge goes a long way

Emerging markets are tempting for businesses but can be risky, uncharted territory for the inexperienced.

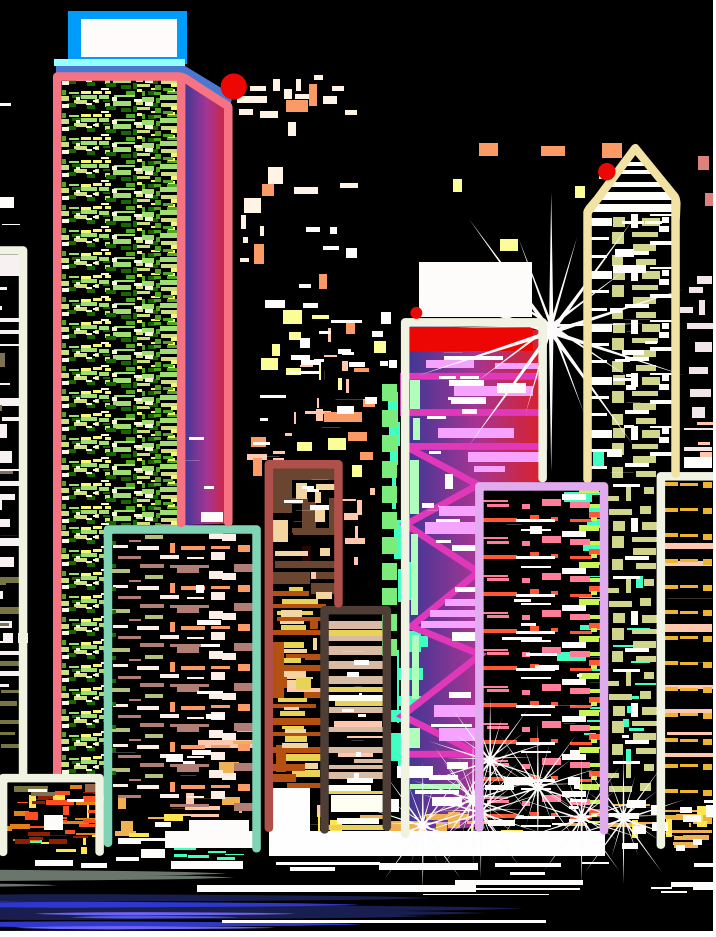
So what happens when one business buys another in a country where it has not previously operated and has no knowledge of the local culture?

The standard procedure might be that a company applies the same due diligence model it uses everywhere else, installs the same standard cyber security it would in the US or Europe and shares the intellectual property the operation requires.

Job done? Yes. Or until a crisis hits. In this situation, it's highly likely that the due diligence model does not capture some unexpected "externalities" such that it is normal practice in the country concerned to pay senior staff in untraceable cash, or to bribe public officials through fictitious subcontractors. Or even something seemingly innocent, such as staff are accustomed to working from home and valuable intellectual property essentially 'walks out the door' to someone's insecure home computer each night.

Preparing to do business in an emerging market means understanding the risks of the environment in order to not only operate, but prosper.

BRIGHT LIGHTS, BIG CITY



KEY FINDINGS

- Survey of 50+ legal professionals (**69%** are director level or general counsel) with operations in emerging markets
- **38.3%** of respondents use a subsidiary in emerging markets, as opposed to **17%** who use a branch structure and **14.9%** who use a joint venture
- **70.8%** of respondents operating in emerging markets use a mixture of local and expat staff
- The most common type of fraud that companies have experienced is: regulatory/compliance breach (**26.1%**); a sizeable quarter of respondents do not even know if they have experienced fraud
- **Nearly half** of respondents prefer to use country specific due diligence, as opposed to standardised due diligence across borders
- **Nearly 40%** of respondents provide English-only whistleblower hotlines in emerging markets due to lack of capacity and ability to provide multilingual assistance
- Information security response plans are rarely tailored to the markets companies operate in, with **30.4%** being unsure of this and **30.4%** saying they are not tailored at all.

A fine line must be walked between assuming that an emerging market is just like the US or Europe and assuming that it is too risky and complicated to pursue any profitable opportunities.

As a survey by *Legal Week*, in association with international corporate investigations and risk management firm Kroll, of more than 50 senior legal professionals (65% of which are director level or general counsel) has shown, some businesses have grasped where this balance lies.

Many though, have not owned up to this reality, suggesting there are still some major pitfalls that firms looking to expand in emerging markets must be mindful of.

EJ Hilbert, head of cyber investigations for Kroll in Europe, the Middle East and Africa and former Federal Bureau of Investigations special agent, sums up the landscape of fraud and cyber security in emerging markets:

"Without trying to fearmonger, cyber security is an enormous threat in emerging markets because it is the primary fraud methodology of the day. There is no need for anyone to do physical intrusion when you can get it all over the wires.

"Bad guys will take advantage of opportunities, and if you don't understand the threats you can't protect against them and, let's be honest, most people don't understand them."

Often, an insecure situation in emerging markets begins where companies least expect it: right at the beginning.

Kroll managing director Zoe Newman, a forensic accountant by background, explains that a major danger is importing cyber insecurity as a result of a business deal.

"One of the biggest issues we see when conducting fraud and corruption investigations, is that a

Continued on page 5

CASE STUDY: EASTERN EUROPE

Kroll was contacted by the regional General Counsel of a multinational who had concerns over payments made within a government contract held by a subsidiary in Eastern Europe. The contract was live, and the issue had been brought to his attention via an internal audit. Specifically, suspicious payments totalling €35m had been made to entities in Europe, the Americas and offshore.

Kroll was retained to conduct a forensic investigation of the contract's history covering a five year period to help establish whether fraud or corruption was involved.

Prior to commencing the investigation, specific issues needed to be considered:

1. Confidentiality - the contract was live and there was a risk of negative publicity;
2. The investigation had to comply with data protection laws in multiple jurisdictions;
3. Multiple languages and cultures;
4. The majority of individuals involved in winning the contract were no longer with the company.

Kroll's forensic accountants worked with the client's internal audit team to interrogate the centralised accounting system from regional head office and identify all revenue and expense payments relevant to the contract. Kroll forensically reconstructed the contract to identify the relevant parties, including employees, customers and suppliers, using both hard copy and electronic data. Over a terabyte of electronic data was collected, discreetly, from multiple jurisdictions after US counsel sought local advice on data privacy laws relevant to each jurisdiction.

Information identified from the analysis was fed into the electronic data review team, who in turn relayed their relevant findings for follow up. The electronic review required local language and cultural awareness, achieved through co-ordination with corporate counsel and Kroll's international footprint.

Extensive external investigative research was conducted in the relevant jurisdictions to understand the legitimacy of suppliers, as well as the corporate interests and political affiliations of current and former employees involved in the contract.

Significant red flags were identified involving third parties' profiles and irregular documentation. These included sequential invoices, round sum and one off payments, websites created just before the contract was awarded and the use of prepayments and shell companies.

Additional suspicious payments to suspect entities were identified through forensic accounting and data mining which led to the scope of the investigation being extended to include other contracts. A follow up email review and additional research found that corrupt local management had seeded a number of entities across the supplier base for their own financial gain. Kroll compiled funds flow analyses and evidential reports relating to the beneficiaries of the frauds, enabling corporate counsel to initiate actions for recoveries.

The results of the investigation led to the client's decision to self-report to the regulators.

The client entered into a significant remediation exercise, designed to implement controls to prevent the reoccurrence of similar events. These included: retrospective risk profiling of its supplier base, taking into account enhanced risk measures in high-risk jurisdictions; a gradual phasing out of the branch structure in favour of subsidiaries; implementation of a whistleblowing hotline in all country locations, in local language, and adaptation of the internal audit cycle and scope to incorporate data mining and country specific expertise.

large corporate might have a robust information security programme in its core western markets, but if operations in emerging markets have been acquired rather than developed organically, the systems there can often be completely different."

Employees: the first line of fraud and corruption defence

But what can be done from the start to prevent this from happening?

Hilbert says the key to keeping an emerging market operation secure is less obvious than some might think. It can be as simple as education: "Companies may put in high end technology, but no one in the emerging market knows how to use it, so they just go back to the old ways," he says.

This may mean spending both time, money and even undertaking some local fieldwork on the emerging market culture, which will pay dividends in terms of security in the long run. In information security, companies need to make sure they invest in the people and help them understand the nature of the business and why certain systems are in place, rather than merely demanding people "work with it."

Hilbert continues: "Educating employees is key. Not only are they your primary threat, they are your primary level of defence and they will see problems first."

This is a two-way process. A major western corporate may be equally ignorant of local culture.

"If you are a security expert who goes to the Middle East your primary concern will probably be corporate data, and very few people will look at personal records," he explains as an example.

"But, in the Middle East, a picture of someone's family can be far more important than a document from a company, and could be used as a threat or for manipulation of an employee to provide information about the company rather than have their personal life exposed.

"If you don't understand those cultural norms, all 'standard' information security measures can be undermined. You need to help people in local markets defend the information they think needs to be protected, and that comes back to education."

Intellectual property: multiple views required

Newman urges companies to consider carefully how to handle intellectual property in emerging markets, as the terrain that will be encountered will almost certainly be different from a company's home market.

"There are huge benefits from operating in emerging markets but it's necessary to assess what is critical intellectual property and where it should be stored," she says. The advantage of going to emerging markets for production may not (for example) outweigh the benefits of safeguarding intellectual property in your home territory.

"One issue is trying to litigate if any problems arise in an emerging market, as once intellectual property is gone, it's very difficult to get an injunction in countries such as China or Russia."

Hilbert agrees: "These are sovereign nations with laws that are not the same as at home. Even if you get an injunction in the UK, who says anyone will acknowledge that in Indonesia or Kazakhstan? Very significant legal and risk analysis must occur before you start investing in these areas."

Physical security of your staff may be integral to the safety of emerging market business. Care must also be taken with the security arrangements of emerging market lawyers and other corporate advisers.

"There has been a dramatic up-tick in cyberattacks on lawyers and accountants because they are seen as the middle men," Hilbert says.

"You may have great corporate security but have to utilise local attorneys and accountants and others so they are targeted for the information they hold on you."

Newman points out: "People do technical cyber security assessments that are OK as of the day they were implemented, but threats evolve all the time and can change."

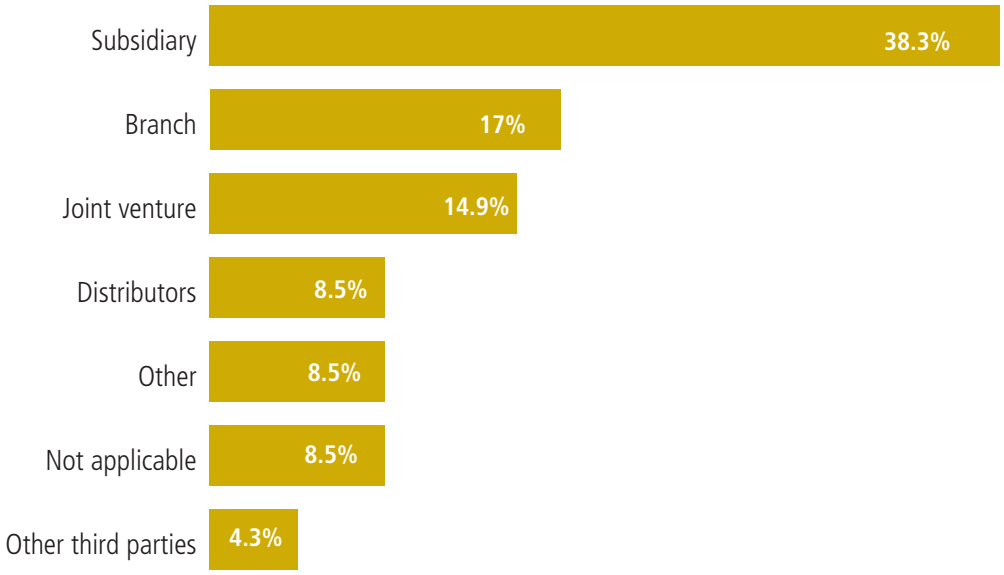
The hottest emerging markets

Legal Week's research showed that respondent companies had operations in many emerging markets, and the most popular places for new operations over the next three years were Eastern Europe, the former Soviet Union outside Russia (where almost

Continued on page 6

"Educating employees is key. Not only are they your primary threat, they are your primary level of defence" EJ Hilbert, head of cyber investigations, EMEA, Kroll

How do you typically operate in emerging markets?



all respondents were anyway established), South East Asia and the Middle East and North Africa.

Newman says firms are "still very wary of sub-Saharan Africa, except South Africa, because it's less developed and bribery and corruption risk can be high.

"Those with planned operations in South East Asia often use Singapore and Hong Kong as hubs because they feel more similar to their home markets, but the opportunities are often more attractive in outlying countries, so make sure you understand the culture of your specific target markets."

How to grow: subsidiary or branch structure?

The survey also found that 38.3% of respondents used a subsidiary in emerging markets, 17% a branch and 14.9% joint venture as the three most common approaches.

The preference for use of the subsidiary structure doesn't surprise Newman, who says: "We see a combination of all three, but subsidiary is the most typical.

"One issue we have seen from corruption investigations is the lack of control that can come with a subsidiary structure."

If, say, a British company has a branch in Bulgaria, there will normally be a level of oversight and therefore control maintained in the UK, whereas a subsidiary has more autonomy.

"Where people have bought a local company they tend to inherit its internal controls, IT system and culture so headquarters can have all-singing and dancing systems in place and great standard operating procedures, but the actual reporting from the subsidiary to group is just an Excel spreadsheet. Anyone can get at that and it's totally reliant on the information that's been entered."

The right blend of local and expat knowledge

Respondents overwhelmingly chose to use a combination of local and expat senior staff in emerging markets, with 71.1% opting for this.

Newman describes this choice as "quite reassuring as in the majority of investigations we've been asked to undertake where things go wrong in emerging markets, it's typically where a company makes an acquisition and leaves incumbents in place to run the business as if it was still their own.

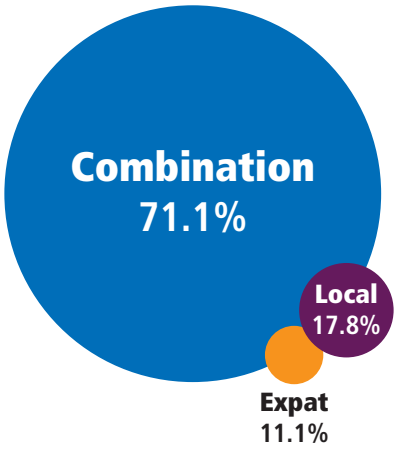
"There is a benefit in that local staff understand the local culture and operating environment, and if you put in expat staff, they need to be able to speak the language."

She suggests regular rotation of local staff to established markets so they can better grasp the corporate culture and points to one 'how not to do it' example.

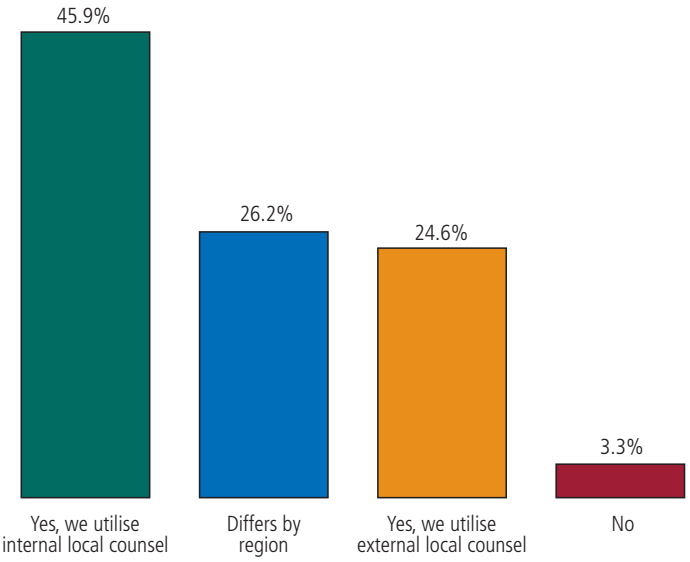
Newman encountered "a case in China where there was a major corruption issue and the client parachuted in someone to manage that operation who didn't speak a word of Mandarin and had 150 staff reporting to them that didn't speak English."

"One issue we have seen from corruption investigations is the lack of control that can come with a subsidiary structure" Zoe Newman, managing director, Kroll

What is your approach to senior staffing?



Do you utilise local counsel in the emerging markets in which you operate?



These local cultural issues coupled with national regulatory ones, make it important to use local counsel, whether internal or external, and all but a handful of respondents did so.

Hilbert says: "Internal general counsel will be extremely busy and will not understand all the issues that may arise and will rely on external counsel."

Corruption is a widespread worry in emerging markets, and there was some surprise that just over a quarter of respondents audited operations there less frequently than annually.

Newman says that while at least an annual audit was desirable, it was equally important to be clear

Continued on page 8

about what was being audited and by whom.

"You can have an internal audit review every month, but if it is done by people who don't know the local culture it's largely pointless," she says.

"Internal audit is not a fraud investigation tool, and it is key to understand local cultural issues so companies are not fobbed off by local managements that blame internal audit when things go wrong."

She points out that where a local management has carried out a dubious transaction the paperwork will ostensibly appear to be in order, so group-level management needs to "have done research to see unusual payments to suppliers, the business affiliations of local managers and use that kind of thinking to spot corruption issues".

Country-specific due diligence v standardised due diligence

Similar suspicions of an over-reliance on 'box ticking' emerged in response to a question on how companies conduct due diligence in emerging markets.

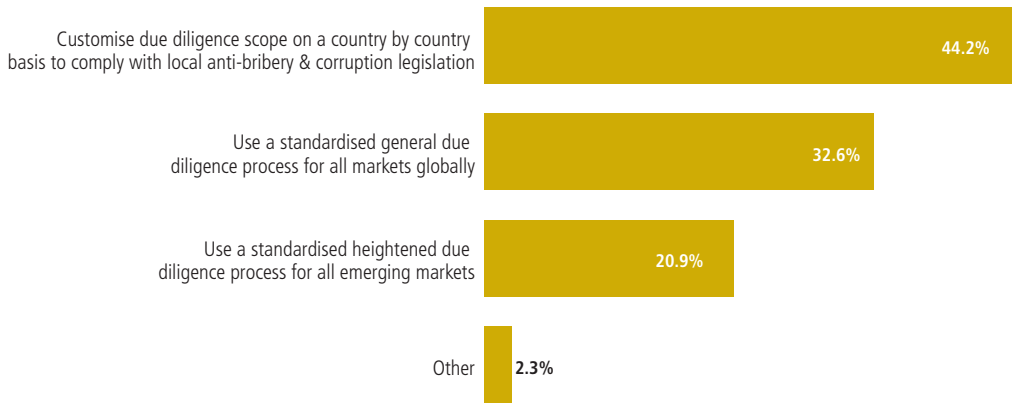
While 44.2% of respondents customise due diligence on a country-by-country basis, the rest used various standardised systems.

Newman suspects that where non-customised due diligence is used, companies may simply look at published data, which can be dangerous.

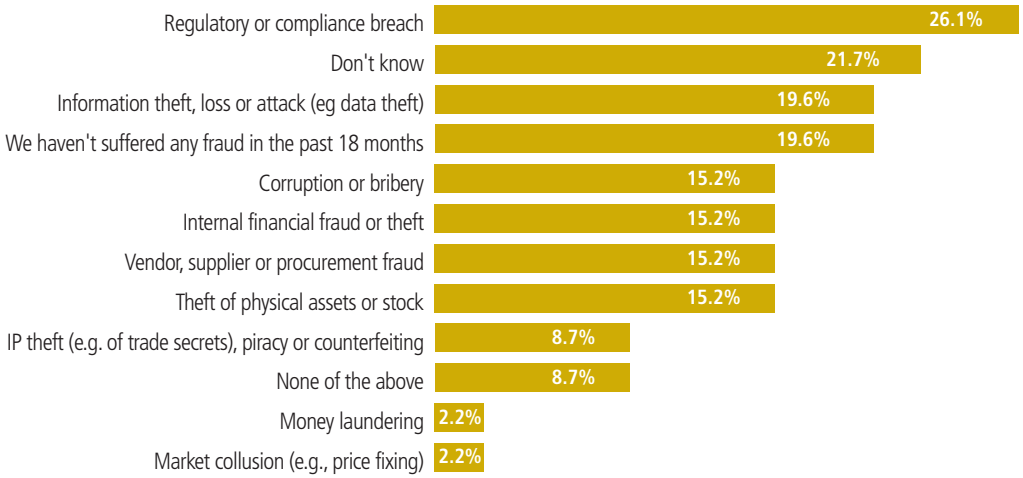
"A lot of corporates just want a 'box-ticking' exercise based on public records but in emerging markets public records can inherently be unreliable and what is in the media can be what people have paid to be put there.

"It is key that someone who understands the local jurisdiction does it, so they can ask questions in the market. A lot of SMEs will not have much public profile, so you need to tap into market rumour and gossip, and in the Middle East and sub-Saharan Africa there is often a lack of any available public record anyway."

When you conduct due diligence on third parties in emerging markets, do you...?



What types of fraud has your company been subjected to in the last 18 months with regards to your emerging market subsidiaries?



The known unknowns of fraud

When it came to considering the types of frauds that companies might have suffered in emerging markets, 21.7% of respondents admitted to not knowing whether or not they had suffered fraud in the past 18 months.

Of those who did know, information or intellectual property theft together accounted for 19.6% of cases and regulatory or compliance breaches for 26.1%, with 15.2% each for corruption, internal fraud and vendor fraud.

Hilbert says frauds are rarely country-specific and "you will get every kind of fraud everywhere".

Despite awareness of the possibility of fraud, when asked

CASE STUDY: CYBER CRIME

A major international energy company had suffered a significant data breach and damage to its IT systems by external hackers who had been inside the company network for three months.

Kroll was engaged to provide investigations expertise and to determine the scale and nature of what had happened, who had done it, and to examine the roles of employees. Kroll was retained by US counsel to maintain legal privilege and confidentiality over our findings.

Prior to starting the investigation, specific issues had to be considered:

1. Confidentiality – there was extensive coverage of the event in the media

2. Data protection – the investigation could not take information out of the host nation without government approval

"The team analysed vast amounts of data to obtain a patchwork of clues that identified the perpetrators"

3. Cultural issues surrounding the location of the breach, including different sensitivities during interviews

4. Political issues arising from the possible involvement of another nation state

Kroll deployed a bespoke team of specialist investigators to assist immediately. We then won court orders in France to disclose ownership details of the key server that was used in the exfiltration.

The team analysed vast amounts of data to obtain a patchwork of clues that identified the perpetrators, and then profiled their international and domestic footprints for law enforcement.

Kroll also clarified the errors and omissions by employees that enabled the breach to occur and recommended changes to procedures and architecture to prevent a reoccurrence.

A full report was provided to the local prosecutor to explain why Kroll did not believe that an insider had been involved.

As a result of Kroll's investigation, the client was confident that it fully understood what had happened and who the perpetrators were.

The client was also able to reassure the Government that the problem had been dealt with appropriately and that new procedures had been put in place to enhance controls and provide a layered defence against any future attacks.

'is your information security incident response plan tailored to every market in which you operate based on local law, regulation and infrastructure?' 30.4% were unsure and 30.4% said 'no'.

"Not knowing the local threats is being foolish," Hilbert says. Global threats are important but most attacks will be based on local groups with local ties.

"If an incident occurs and the security plan is inadequate, whoever is in charge of security is ultimately responsible."

An almost equally startling level of ignorance appeared in answers to: 'Where do you host client data for your emerging market subsidiaries?' with 17.4% answering 'don't know', while 26.1% kept it in the country concerned, 37% in the EU or US, 10.9% 'other' and 8.7% with a non-geographical location specific cloud provider.

Hilbert points out that: "A cloud is not non-geographic, it's on someone's server somewhere."

Emerging market governments may have rules that data is stored locally but "it becomes a threat as someone may take it, or you give it to a third party in that jurisdiction and you do not know what security they have".

Newman says that if data is hosted in an emerging market an investigation into fraud may be hampered as "a lot of emerging markets jurisdictions prevent you taking it out, and may have stricter data protection laws than in UK.

"In an investigation I was involved in, data had to be left with a local law firm for six months while we navigated the local legal landscape to enable lawyers in US to review it. Even massive multinationals try to save server and storage space by encouraging employees to back up emails to hard drives, and when something goes wrong everything is on them

Continued on page 10

and you cannot just lift a copy from head office."

Whistleblowing: a deterrent in many languages

Whistleblowing can be an effective way to uncover fraud but Hilbert says it works best in the few countries such as the US where the whistleblower benefits directly from detected frauds. Newman notes that its effectiveness is blunted in some countries where "deference to seniority means they will rarely blow the whistle; it comes back to local management and culture".

Among respondents, 39.1% provided whistleblower hotlines in English only, which Hilbert speculated was because companies did not have the capacity centrally to act on reports in local languages.

Despite these problems, whistleblowers accounted for 34.7% of fraud reports, with 25% coming from local managements and another 26% from audits.

Newman pointed out a possible reason for the relatively low levels of reports from managers: "For a significant fraud to occur in markets there usually has to be some implicit involvement of local managements so they will be less likely to report it."

Self-reporting on corruption or bribery to an emerging market's regulatory body was extremely rare, with just 8.3% having taken this step.

Hilbert says: "In many cases, local authorities should at least be notified so that you have a report with a legal entity that you can refer back to if you take legal action.

"However good local police may be, specialist advice will be needed because police will be fully occupied with their normal tasks and may view fraud against a foreign company as less pressing than their duties towards local citizens."

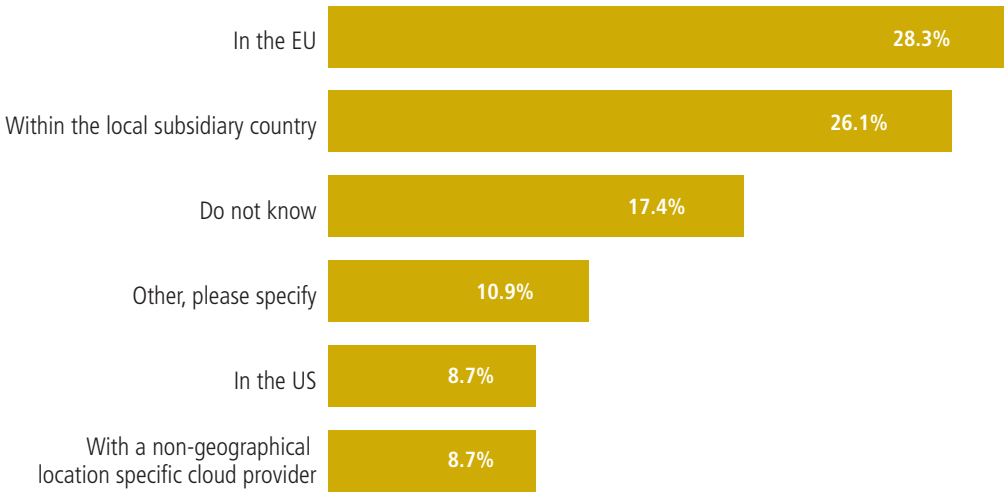
Newman expects self-reporting to "vastly increase" in the next five years as countries seek to improve their reputations as places to do business by implementing anti-bribery and corruptions laws, making it a requirement.

Hilbert says local regulations will generally tighten, as "countries do not want to be known as the place where you cannot send any of your intellectual property".

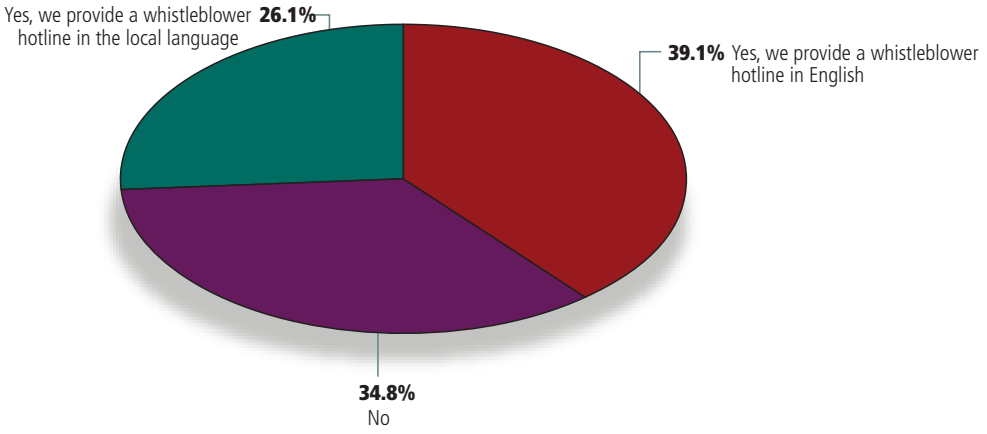
Local economic growth may also lessen cyber insecurity, which is at present notably prevalent, he says, where "there is a wealth of computer knowledge and a limited market for individuals with that skill set. The threat is there if there are no jobs comparable to their skills; they are going to go onto the web and find a way to make money."

Security concerns should not keep any company out of emerging markets altogether, but the precautions needed – whether in due diligence, audit or security arrangements – all essentially come down to understanding what is going on, or might do so, in the country and culture concerned, and planning accordingly.

Where do you host client data for your emerging market subsidiaries?



Do you provide a whistleblower hotline in your emerging markets subsidiaries?



VIEWPOINT: HOW TO TACKLE DUE DILIGENCE IN A NEW JURISDICTION

Two senior lawyers used to dealing with the pitfalls of emerging markets are Ian Stoodley, deputy general counsel at Intel Capital, and Jeremy Barton, general counsel at Boston Consulting Group.

Both companies are, they say, in the happy position of not having suffered fraud in emerging markets.

Having seen the survey results, Stoodley says: "When you approach a transaction in a different jurisdiction you have to start with the macro environment in the country. To take one small example, corporate governance in the UK and US places great reliance on independent non-executive directors, whereas in many emerging markets it is not uncommon for family members or close contacts to be on a board or involved with a company. It's just a different view and it's important to try and understand the perspective of people that you are negotiating with."

Intel Capital has a global programme of making minority investments and, having invested in 54 countries to date, has practical experience of many emerging market companies with growth potential. Stoodley uses Transparency International and other published data for risk rating "as a starting point for the due diligence process. When assessing the risk of bribery and corruption in any potential investment, we look not only at location but also a number of key factors such as the amount of revenue the target derives from the public sector and the extent to which it uses third party agents or consultants".


Ian Stoodley

Barton says Boston Consulting Group "tends to apply a global test which we do believe is robust enough to cope with issues.

"People tend to assume that risks of fraud and corruption in emerging markets are worse than elsewhere, but you need to be vigilant in any market.


Jeremy Barton

"There is also a perception that regulation in emerging markets is either lax, or is some something strange and like nothing else on Earth. In fact while it may not be as developed as elsewhere, it's often based on some well understood regime."

Boston Consulting Group will tailor its cyber security to the country concerned, and in some places staff are given only desktop computers to prevent any data leakage from laptops that could be easily removed from its buildings. All the company's IT is centralised both for ease of operation and security.

Its whistleblowing policy is solely in English "but that is the working language of the business and people are encouraged to raise concerns, though there are some countries that are very hierarchical where raising concerns about a superior is difficult," he says.

"People tend to assume that risks of fraud and corruption in emerging markets are worse than elsewhere"

- Fraud
- Bribery & Corruption
- Information Security & Cyber threats
- Asset Tracing & Recovery
- Litigation Support
- Dispute Resolution
- Forensic Accounting
- Transaction Intelligence

Your Global Investigations Partner

Kroll's Investigations team contains a unique mix of specialised skills. We work in small multi-skilled teams to deliver customised investigations which produce evidence that meets the highest litigation standards. Around the world we enable our clients to make informed decisions about their most difficult challenges.

Our team includes intelligence gathering, law enforcement,accountancy, data analytics and cyber investigation expertise.

+44 (0) 207 029 5000 | KrollUK@kroll.com | www.krolladvisory.com

Kroll®