Investigating procurement fraud in South and Southeast Asia

By Reshmi Khurana & Stefano Demichelis

With their distinctive characteristics and cultural nuances – not to mention business etiquette standards that vary from country to country – markets in South and Southeast Asia can pose unexpected challenges for companies that rely on fraud mitigation and investigation practices applicable to developed markets. Quite simply, these practices do not work in Asia. In fact, some common Asian business practices make companies more vulnerable to fraud, especially procurement fraud, and at the same time make it harder for investigations to be carried out.

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.
- **External and Internal Leads.** Interview internal process owners and second tier employees. Coordinate external source inquiries to provide additional investigative leads and keywords.

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

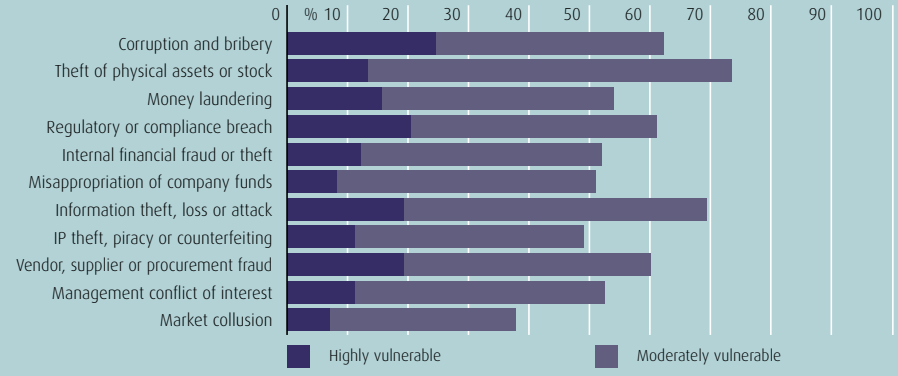
In the event of a suspected fraud when targets are unknown, Kroll works to isolate the source of the problem by:

- 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:
  - Building secure environments that reduce the risk of access control systems' being compromised
  - Conducting due diligence on new employees and vendors
  - Instituting anonymous and independent whistle-blowing systems that encourage local employees and vendors to report unethical behavior while protecting them from direct and indirect punitive actions

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.

FINANCIAL SERVICES — ECONOMIST INTELLIGENCE UNIT REPORT CARD

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 the 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.



Loss: Average percentage of revenue lost to fraud: 1.5%

Prevalence: Companies affected by fraud: 75%

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%)

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

Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected: IT complexity (47%)

Reshmi Khurana is the head of Kroll's India office. Reshmi has more than 13 years of experience conducting complex corruption investigations, litigation support, and due diligence on the management, operations and business models of organizations across the US, South Asia and South East Asia. Her clients include asset management companies, corporations in the mining, oil & gas, consumer packaged goods and pharmaceutical industries and law firms.

Stefano Demichelis is an Associate Managing Director for Kroll based in Singapore. Stefano has extensive experience providing support to clients for prevention, detection and investigation of fraud. His experience includes investigating payroll fraud perpetrated by a supervisor that resulted in a loss of Euro 3.5m; investigating the identity theft of a Hedge Fund owner; implementing automated tests in an hotel chain for the identification of credit card fraud perpetrated by front desk employees.