

Asia a happy place for frauds

Michael Backman
THE AGE
February 14, 2007
Page 1 of 2

SELLING business services in Asia is difficult. The region's business people largely are descended from Chinese middlemen traders of goods.

And so there remains limited appreciation of the value of services, either as something to be sold, or as business inputs. This means services such as legal, accounting, staff training and marketing tend to be under-acquired.

But, increasingly, business services providers are plying their trade in Asia. Most start out consulting to other foreign companies operating in Asia. For example, British PR consultants in Shanghai will work mostly for the China offices of big British companies. From this they can hope to develop local clients.

Many companies involved in supplying business services in Asia have Australian links. One, the Insight Risk Group, founded in Singapore by Paul Curby, a former NSW policeman, offers companies fraud risk management, fraud investigation, due diligence work, computer forensics and forensic document analysis.

One might imagine the scope for this sort of work to be almost limitless in Asia: the rule of law often is weak and regulatory agencies are underfunded and ill-trained. The global Association of Certified Fraud Examiners (ACFE) estimated last year that worldwide, 5 per cent of corporate revenue is lost to fraud. How much greater this figure must be in Asia with its lax controls? Another estimate is that up to 70 per cent of fraud goes undetected and is wrongly assigned as credit losses.

As a former attorney-general of Indonesia said, Indonesia cannot afford to enforce its white-collar crime laws fully because, if it did, most of Indonesia's business community would end up in jail.

Asian companies obviously have a lot to gain by buying-in a fraud control service. But most of Insight Risk's clients are still multinationals. Curby is critical of the internal fraud control measures of even Asia's better-managed banks. Many believe their internal and external audit processes are sufficient to detect irregularities.

He cites a recent talk with a senior manager of a well-known local financial institution. The manager mentioned that he knew that organised crime groups were soliciting information from his staff and former staff to detect weaknesses to be exploited in the institution's processes.

The manager insisted that Curby must have some software to run across their system to fix the problem. And so yet again, Asia's self-defeating distaste for paying for professional services revealed itself.

Banking in Asia is particularly ripe for fraud. Financial institutions are grappling with regulatory changes from all directions as the region's regulators aim to improve governance so another region-wide collapse of the ilk of the 1997-98 Asian financial crisis does not happen again.

But doing a deal emanating in Hong Kong can have regulatory implications in Singapore. Compliance functions have grown. And a lot of energy must go into keeping transactions within the regulatory framework.

Further weaknesses arise when banks use multiple systems to process a transaction. Banking mergers exacerbate the problem.

Malaysia, for example, recently required its 54 financial institutions to merge to form just 10 banks. Such mergers generate cost savings from greater economies of scale, but also introduce conflicts between systems and confusion among staff during the initial period. Fraudsters can exploit all this.

Product innovation also may cause opportunities for weaknesses and fraud. To cope with product offerings, banks may move from straight through processing (STP) one year to manual inputting the next, for example.

But what precisely are the weaknesses? Curby and his colleagues find out by interviewing staff. Staff who input or process transactions have close knowledge of their company's systems and processes.

As Curby says, this is true of any organisation but it is a factor that is often overlooked: it is the staff who usually are the experts in how their company could be defrauded.

The staff involved are given a suitable briefing beforehand. They are reminded that they are not being involved in a fraud investigation or an audit but a risk-management exercise. Curby and his colleagues then work with the staff to identify fraud schemes that may go undetected in the control environment.

The controls are then "stress" tested and a worst-case dollar loss scenario is developed, along with the impact on the business from regulatory and reputation perspectives.

Of course, no company deliberately employs potential fraudsters, but the 20-year-old employee that it recruits is not going to be the same person at 30. And people's circumstances change.

Statistics compiled last year by the ACFE showed that more than 60 per cent of fraud perpetrators had been with their companies for more than five years and almost 40 per cent for more than 10 years. More than 60 per cent were found to have acted alone.

Rarely is fraud a one-off. Initial perceived need typically turns to greed. Singapore Airlines was defrauded of \$35 million over more than 13 years. The perpetrator was jailed in 2000. In 2004, the finance manager at Singapore's Asia Pacific Breweries was jailed for stealing \$117 million over four years. The Singapore Airlines example is particularly noteworthy because early in his career the perpetrator noticed a weakness in the company's processes. He brought it to his manager's attention but was ignored.

<http://www.theage.com.au/articles/2007/02/13/1171128974132.html>

michaelbackman@yahoo.com

www.michaelbackman.com