Procurement fraud a growing economic crime

Greater competition in tender process among factors driving procurement fraud in Malaysia

by Amy Chew

PRESSURING suppliers to pay kickbacks and helping family members become vendors are typical incidents of procurement fraud suffered by some 19% of Malaysian businesses, including government-linked corporations (GLCs) this year, according to global accounting firm PricewaterhouseCoopers (PwC).

Greater competition in public tender process from government and state-owned businesses are among factors driving procurement fraud in the country, an issue which anti-graft watchdogs have long warned and campaigned against.

"Most of the procurement fraud investigations that we have undertaken involve either private sector companies or, in some cases, GLCs," Alex Tan, executive director and forensics lead of PwC, tells ***FocusM***. Tan has over 20 years as an investigator, including nine years with the Royal Hong Kong Police Force and eight years with the New Zealand Serious Fraud Office.

PwC recently released its biennial 2014 Global Economic Crime Survey conducted across 15 different industries including the financial services sector and government and state-owned enterprises.

In the report, procurement fraud was added as a new category as it is viewed as specific area of risk. "We believe this category is primarily driven by two trends – more-competitive public tender processes from governments and state-owned businesses, and the increasing integration of supply chain into core business activities," says Tan.

"With respect to procurement fraud in Malaysia, the typical type that we see is either staff providing opportunities to friends and contacts, or staff putting pressure on existing suppliers to pay kickbacks," he adds.

There were also incidents of senior staff members helping family members to become vendors, says Tan.

PwC warns it is important not to overlook the threat from within in dealing with procurement fraud and that no industry is immune. From PwC's experience, if an organisation purchases goods and services, it is an area ripe for fraud.

"We have seen a number of instances where an employee provides information on the bidding process such as budget or bid amounts of competitors to ensure an advantage for their preferred bidders," according to the survey.

"We have even seen instances where staff have helped vendors complete tender documents or instructed vendors to provide 'dummy' quotes," says PwC.

In the survey, 50% of the respondents said procurement fraud had occurred during vendor selection, and 33% said it occurred within the bid process, vendor maintenance and payment processes.

Procurement fraud, says PwC, victimises organisations in their acquisition of goods and services. It also prevents companies from competing fairly and successfully for business opportunities.

To reduce incidents of procurement fraud, it is crucial for "handlers" of a tender process to be persons of integrity, according to anti-graft watchdog, Transparency International Malaysia (TI Malaysia).

"You need to have a good system and a handler with high integrity, only then can you prevent corruption during procurement," says TI Malaysia president Akhbar Satar.

> **"In respect to procurement fraud in Malaysia, the typical type that we see is either staff providing opportunities to friends and contacts, or staff putting pressure on existing suppliers to pay kickbacks."**
>
> – Tan

Cybercrime on the rise

Cybercrime is also emerging as a serious economic crime, having spiked 31% this year from 5% in 2011. This is above the global average of 24%, according to the survey. Of this, 9% of these believed they suffered financial losses of more than US$1 mil (RM3.27 mil).

Cybercrime in Malaysia resulted in losses totalling RM84.3 mil in 2013, according to the Royal Malaysian Police (PDRM).

"Apart from banking, other sectors also contributed to the figure, ie hacking, phishing, spoofing, parcel scams, love scams and online purchasing," Assistant Police Commissioner Ahmad Nordin tells ***FocusM***.

PwC warns that the banking sector is the main target for cybercrime but no sectors are immune.

"The financial sector is currently the main target as that is where large amounts of money are held. As the financial sector tightens its cybercrime prevention methods, cyber criminals will shift their focus to other sectors," says Tan, adding the financial sector, by and large, is taking very active steps to mitigate cybercrime risks.

Amongst the modus operandi of cyber criminals is creating false identities which are then used to commit wide-ranging crimes such as fraud, money laundering and terrorism, he explains.

"Cybercrime is a young person's game. Our Malaysian business is underestimating this," says Tan.

In some cases, senior management and board members may not fully grasp some of the new technologies being developed and may not be users of social media. "This could present a knowledge gap that fraudsters will look to exploit," warns the survey.

Other examples of cybercrime are instances where an employee accessed a company's server and copied confidential and proprietary information to a storage device or emailed it out from the company and passed it to third parties.

These third parties use the information to either set up a competing business or assist in their own bidding process.

"Needless to say, the potential commercial losses can be significant," says the survey.

Many entities do not have clear insight into whether their networks and the data contained therein have been breached and do not know what has been lost or its value.

Further complicating the picture is the lack of transparency into cybercrime events; even when it is detected, cybercrime often goes unreported.

In some cases, there may be compelling competitive reasons for organisations to keep such losses confidential. "For example, if a confidential bid planning document were accessed by cybercriminals and utilised by rivals to gain an advantage, would a company disclose the incident," the survey asked?

From a commercial point of view, good security requires people to remain focused on their most important data. Companies that inventorise and prioritise the data on their networks are able to focus on the "crown jewels" and spend their limited cyber security budgets wisely, says the survey.

Prevalence of asset misappropriation

Asset misappropriation – the unlawful taking of assets, including monetary assets, cash or supplies and equipment by directors, others in fiduciary positions or an employee, for their own benefit – is the most prevalent economic crime in Malaysia and around the world.

Of the total respondents who said they suffered some form of economic crime in the last two years, 65% said this involved asset misappropriation.

The survey also revealed many organisations in Malaysia do not undertake preventive measures or are not aware of the risks they face from economic crime. In fact, 16% of the respondents say they did not know if they had suffered a single economic crime in the last two years.

"Many organisations appear to believe that their current policies and procedures together with some internal audit reviews are sufficient. Also, many believe that if they are not aware of an incidence of fraud occurring, then fraud is not taking place and so therefore their controls must be working," says Tan.

"Unfortunately this is not always the case," he says.

Tan also says organisations need to undertake fraud "health check" known as fraud risk assessment.

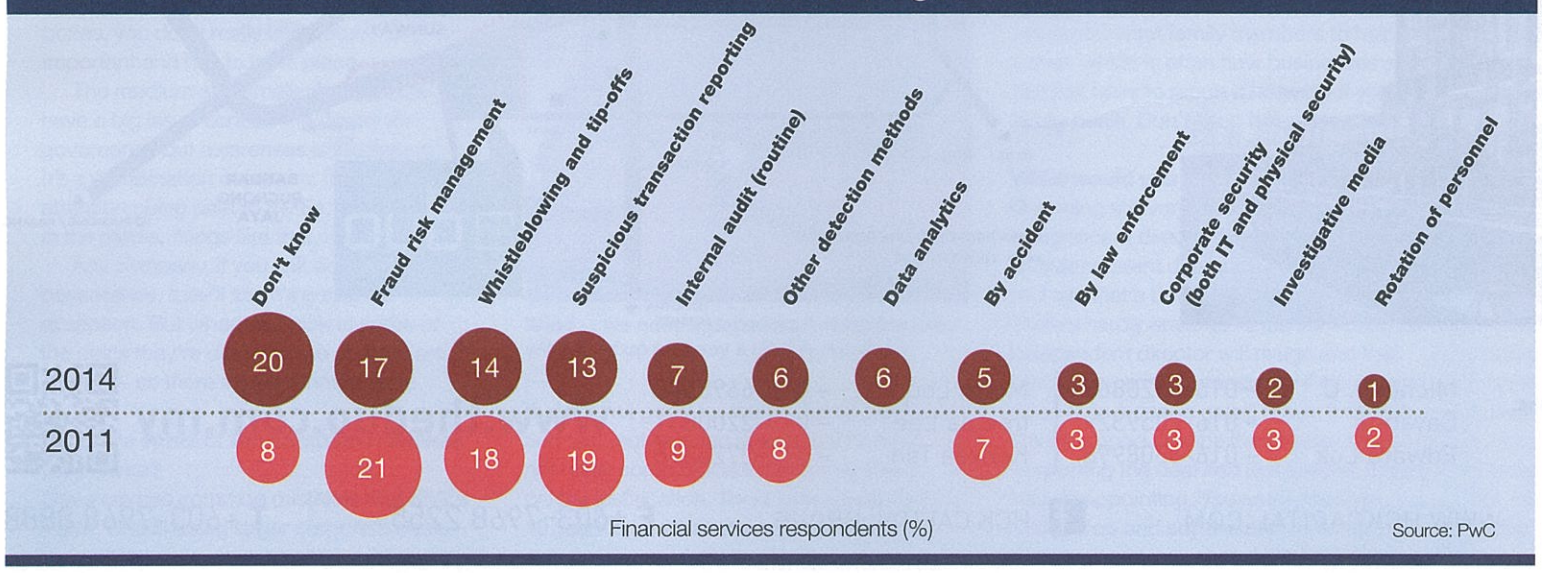
Fraud risk assessments are used to ascertain whether an organisation has undertaken an exercise to specifically consider fraud risks to which operations are exposed; an assessment of the most threatening risks; identification and evaluation of the controls (if any) that are in place to mitigate the key risks; assessment of the general anti-fraud programmes and controls; and actions to remedy any gaps in the controls.

Malaysian companies also appear to be unclear over the impact of corruption on their business.

"Some respondents do not have a clear picture of how corruption may be impacting their organisations either through being asked to pay a bribe or losing business to someone else who did," says the survey.

Undertaking an assessment of corruption risks in a company and having a whistleblower hotline would help prevent and detect economic crimes, says PwC. FocusM

Economic crime detection methods in financial services organisations



Financial services respondents (%)

Source: PwC