

Economic crime: people, culture & controls

The 4th biennial Global Economic Crime Survey
Singapore

Introduction

PricewaterhouseCoopers (PwC) is pleased to present Singapore’s results of the fourth biennial Global Economic Crime Survey.

The 2007 Global Economic Crime Survey was conducted in collaboration with the Economy & Crime Research Center, Halle & Berlin, Germany. The survey was based on interviews with 5,428 executives globally, 894 of whom were from the Asia-Pacific region, and 76 of whom were Singapore-based.

Our survey reveals that fraud remains one of the most problematic issues for businesses worldwide. While companies continue to develop systems and controls to detect and deter economic crime, fraud controls alone are not enough. An ethical corporate culture plays an equally important role in deterring fraud.

Companies in Singapore are riding the wave of rapid economic growth, bringing with it a heavy reliance on technology and fierce competition. However, these

opportunities for growth also present some of the greatest challenges in detecting and deterring fraud.

As our survey clearly shows, it is impossible to get rid of economic crime and there will never be a simple solution, but we endeavour to develop our understanding and share our knowledge of “what works and what does not” in combating fraud.

PwC’s 2007 Global Economic Crime Survey will contribute significantly to the public discussion of economic crime, the development of the ever improving prevention and detection measures, as well as the implementation of an all important corporate culture of zero tolerance towards economic crime.

Fraud – a most problematic business risk

Our 2007 survey reveals that 19% of companies in Singapore have been victims of economic crime over the past two years. This is an increase from

the 16% reported in the 2005 survey. In the Asia-Pacific region, the levels of economic crime has remained unchanged at 39%. Globally, reported economic crime showed a slight decrease from 45% in 2005 to 43% in 2007. (See Table 1)

Considering the significant investment that companies have made in fraud controls over the past two years, why did the levels of economic crime not show a dramatic decrease? In Singapore, our survey shows that incidents of economic crime have actually increased.

This result may be due to what we call a “Fraud Controls Paradox”. Intuitively, it would be reasonable to expect that as companies implement better and stronger controls, the number of frauds detected will drop. However, this may not necessarily be the case in the short term as an increase in controls may lead to an increase in the number of frauds detected. Over time, the gap between the number of detected and undetected cases will narrow as potential fraudsters will become more aware of controls that are in place which means an increase in the risk of them being caught.

Table 1: Companies reporting fraud

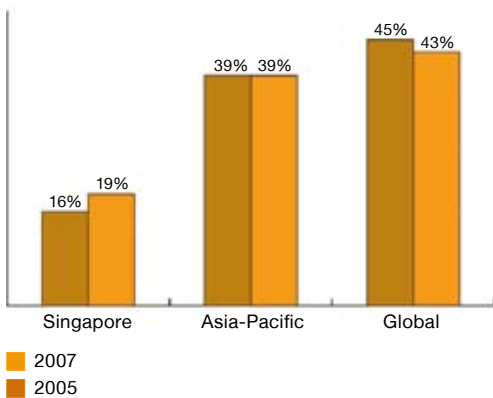
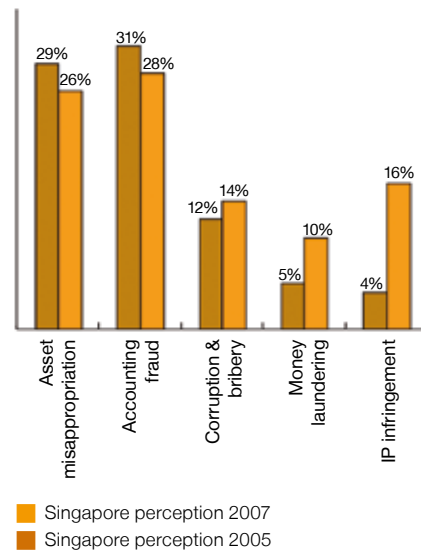


Table 2: Perceived prevalence of fraud



The changing awareness of fraud

In 2005, Singapore companies surveyed perceived asset misappropriation (29%) and accounting fraud (31%) as the two most prevalent types of economic crime as compared to corruption and bribery (12%), money laundering (5%) and Intellectual Property (IP) infringement (4%). The 2007 results suggest that this perception is changing. While asset misappropriation and accounting fraud continue to remain high on the list of most prevalent economic crimes, both registered a drop to 26% and 28% respectively in the 2007 survey. On the other hand, IP infringement, money laundering and corruption and bribery saw increases compared to 2005 – 16% of Singapore companies surveyed said that they consider IP infringement as one of the most prevalent types of economic crime while corruption and bribery and money laundering saw an increase to 14% and 10% respectively. (See Table 2)

The ebbs and flows of this perception index are driven by many factors – from

an increase in global business activity to an increase in the awareness of the specific type of fraud. In the case of IP infringement, the Singapore results show a four-fold increase in the perception of the level of risk of this type of fraud. The reason for this may be the greater awareness of the lack of IP protection as Singapore companies expand abroad and the increase in cases reported in the media of grey market activities, counterfeit goods and illegal software downloads.

Means of detecting fraud

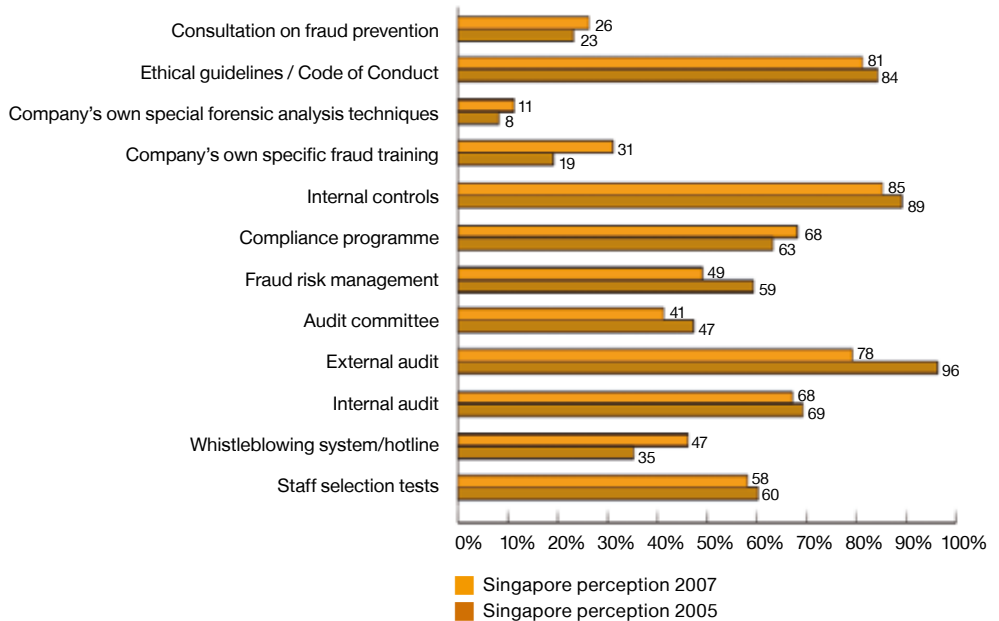
Our results show that Singapore companies and those around the world continue to do more to combat fraud. The average number of discovery and prevention measures for Singapore companies increased from 8 in 2005 to 8.4 in 2007 while Asia-Pacific results record an average of 9 in 2005 and 9.7 in 2007 and global results record an average of 8.5 in 2005 to 9 in 2007.

While the overall number of measures has increased, there has also been a

marked increase in certain specific types of preventive measures since 2005. Most notably, the implementation of a whistle blowing hotline by companies in Singapore increased from 35% in 2005 to 47% in 2007. The organisations surveyed also reported an increased use of their own specific fraud training – from 19% in 2005 to 31% in 2007 – which reflects our experience with clients taking a keen interest in this form of economic crime prevention.

The survey results also revealed a decline in the reliance on external auditors to discover and prevent acts of economic crime. This may reflect companies' increased awareness that fraud prevention and detection is not the main purpose of a statutory audit. In 2005, 96% of Singapore respondents believed external auditors to be one of the main measures to prevent and detect fraud as compared to only 78% in 2007. This is consistent with the global trend, where 96% of the 2005 respondents felt that external audit was one of the main measures to prevent and detect fraud compared to 87% in 2007. (See Table 3)

Table 3: Main measures for the discovery and prevention of acts of economic crime



On the effectiveness of the discovery and preventive measures implemented, our respondents continue to rate the whistle blowing hotline as one of the most effective measures for controlling economic crime. Other measures which were rated highly include internal audit, fraud risk management, in-house forensic analysis techniques and fraud training.

As the business environment is an ever-changing landscape, one can never predict which, if any, of the controls will be effective in detecting and/or preventing fraud.

Globally, we compared companies' current effectiveness in detecting fraud with their collective performance in our previous survey. The results show continued evidence of the intractability of fraud and its apparent immunity to management's attempts to control it. We observe the consistently higher rate of detection through whistle blowing (8% of the cases) or tip-offs (from an internal source in 21% of the cases and from an external source in 14% of the cases). It is our view that this is a result

of employees being encouraged and facilitated to do the right thing – which is a function of culture as opposed to control. (See Table 4)

From fraud detection to fraud prevention

As fraud involves deceit as a fundamental element, it remains difficult to detect. Our research shows that a company that is susceptible to fraud not only lacks sufficient controls to detect fraudulent activities but also lacks ethics, values, programmes and systems that discourage fraud, i.e. corporate culture, including systems that encourage and protect employees who denounce it.

Controls alone will never be sufficient to combat economic crime. Controls, together with an ethical corporate culture that supports a holistic compliance programme working in conjunction with a clearly understood code of ethics, play a defining role in the prevention and detection of fraud.

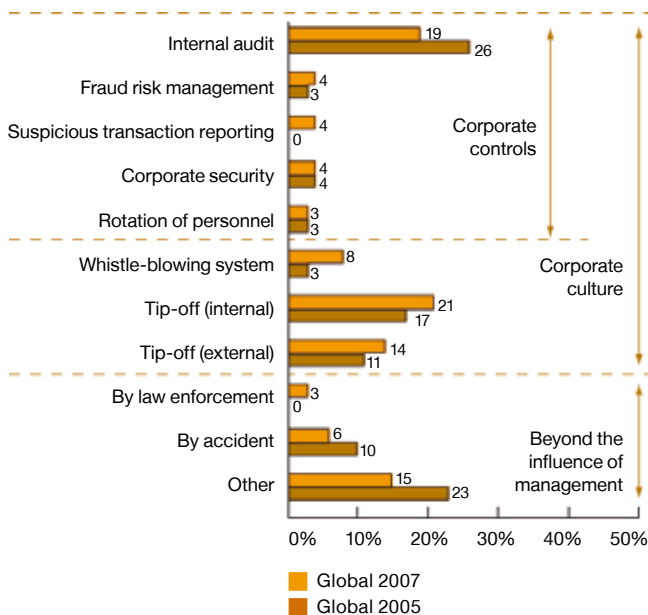
Globally, our 2007 survey shows that companies with both ethics and compliance programmes report fewer economic crimes. Key to the effectiveness of compliance and ethics programmes is not only receiving the correct professional advice on the right types of compliance and detection programmes, but also ensuring that the company ethics guidelines are workable, liveable, and incorporate the explicit norms of criminal law. (See Table 5)

Dealing with fraudsters

An important step in creating a strong ethical corporate culture that does not tolerate fraud is to ensure consistency in actions taken when an economic crime is detected. Most staff are deterred from committing crime when they understand the consequences of their potential foray into fraud and that detection is likely, due to the sophisticated and effective nature of the risk management systems.

The global results indicate that, when a fraud was perpetrated by someone

Table 4: Detection methods



outside of the company, it was reported to a regulator in 38% of the cases, and to law enforcement officers in 64% of the cases. However, when perpetrated by an employee, the incident was reported to regulators in only 24% of the cases, and to law enforcement in only 55% of the cases. From our investigations experience, this also holds true in Singapore where companies are less willing to pursue wrongdoers and report wrongdoings to the relevant authorities but choose rather to “settle the matter” internally.

Based on our survey, despite the fears of negative publicity for involving law enforcement, the companies that referred fraudsters for prosecution, whether internal or external, suffered no significant collateral damage. In fact, in many cases, companies saw a decrease in the collateral damage to their public relations, business relations and their own working morale. A positive response is given by stakeholders and staff when they see consistent, honest and fair action against those who have contravened the company’s ethical guidelines.

We have identified specific, easily-identifiable factors that create the kind of environment in a company that can erode the positive influence of culture:

- Unrealistic pressure on employees to perform or produce
- Absence of clearly defined channels of communication for employees
- Inconsistent action against fraudsters, i.e. senior managers who perpetrate fraud “get off lightly”
- Lack of reporting of economic crimes to authorities

As executives set the tone at the top on the desired corporate culture in an organisation, they have to demonstrate leadership by practising what they preach and this includes acting with integrity as well as taking tough and consistent action against wrongdoers.

Fraud in the future

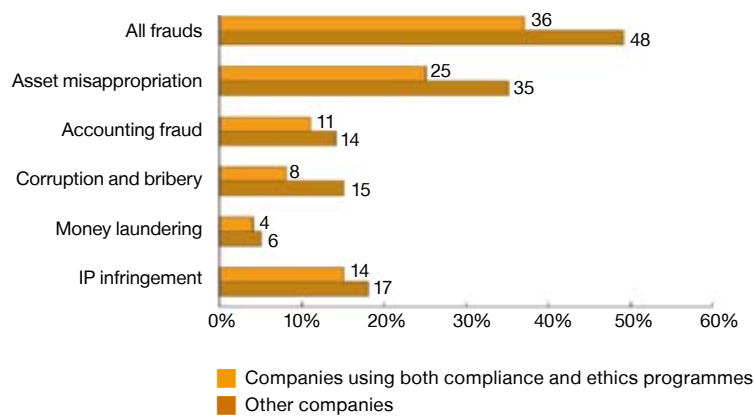
Fraud has always been, and will always be, a real threat. Levels of economic

crime have not dropped over the course of this decade and companies continue to be confident - as they have with every study that we have conducted – that their controls will limit their exposure to fraud in the future.

However, as our survey has shown, controls alone will not be sufficient in mitigating the risk of fraud. Instead, companies with an established culture that supports those controls with clear and ethical guidelines have a better chance at fraud prevention.

The fight against fraud is a constant struggle. Our 2007 survey continues to show that in order to assess and manage risk, a constant re-evaluation of all fraud risk management activities and a culture that supports this in every market of operation is vital to maintain a clear competitive advantage and stakeholder confidence. As with all crimes and unwanted business risks, a move from after-the-fact detection and reaction to consistent and effective prevention is the most valuable move a company can take.

Table 5: Number of economic crimes reported by companies using both compliance and ethics programmes compared to those who do not



Definition of fraud terms used in the PwC Global Economic Crime Survey 2007

- **Fraud/Economic Crime:** The intentional use of deceit to deprive another of money, property or a legal right.
- **Asset Misappropriation (inc. embezzlement/deception by employees):** The theft of company assets (including monetary assets/cash or supplies and equipment) by company directors, others in fiduciary positions or an employee for their own benefit.
- **Accounting Fraud:** Company accounts are altered or presented in such a way that they do not reflect the true value or financial activities of the company.
- **Corruption & Bribery (inc. racketeering and extortion):** The unlawful use of an official position to gain an advantage in contravention of duty. This can involve the promise of an economic benefit or other favour, the use of intimidation or blackmail. It can also refer to the acceptance of such inducements.
- **Money Laundering:** Actions intended to legitimise the proceeds of crime by disguising their true origin.
- **IP Infringement (inc. trademarks, patents, counterfeit products and services, industrial espionage):** This includes the illegal copying and/or distribution of fake goods in breach of patent or copyright, and the creation of false currency notes and coins with the intention of passing them off as genuine. It also includes the illegal acquisition of trade secrets or company information.

Whistle Blowing Programmes: Best Practice Tips

- Safeguard employees who report misconduct against any form of retaliation (i.e. threats, harassment and demotion). Allow for anonymous reporting.
- Make sure employees can report incidents outside their chain of command – avoiding their supervisor, department head and division leader – by using a helpline, e-mail or mail box.
- Maintain confidentiality to the fullest extent possible.
- Ensure that any hotline or helpline is toll free and includes as many language translations as appropriate to a company with global operations.
- Establish working relationships and protocols with various departments within the organisation prior to issues surfacing. For example, Human Resources or Benefits to address personal issues and Security or Risk Management for more serious issues such as suspected fraud.
- Include controls for targeting certain situations which may require immediate steps to prevent further risk or damage.
- Provide clear governance expectations about how matters will be reported to the governing authority, presumably the Board of Directors, or sub-committee.
- Formalise processes for recording and tracking reported issues and incidents.
- Communicate information about the reporting and investigation process, how it operates, what kinds of issues have arisen and how they were dealt with.
- Establish communication channels for not only reporting misconduct, but also for asking questions and receiving guidance.
- Track trends which may appear in one business or across businesses or at specific levels within the organisation.
- Assign appropriate people with both the requisite authority and experience to perform the investigation.
- Establish a company code of conduct that requires all leadership, senior management and employees to fully cooperate in any investigation into allegations of misconduct.
- Establish and consistently enforce a disciplinary policy. A programme that does not abide by its own rules, from the top down, will never work effectively.
- Train and periodically update all employees about the whistle blowing programme, disciplinary policy and the company's code of conduct.

Contact

Dispute Analysis & Investigations Practice

Subramaniam Iyer, Partner
+65 6236 3058
subramaniam.iyer@sg.pwc.com

Chan Kheng Tek, Partner
+65 6236 3628
kheng.tek.chan@sg.pwc.com