

Investigations and Forensic Services

# Economic crime: people, culture & controls

The 4th biennial Global Economic Crime Survey  
India





## Foreword

We are pleased to present the 2007 PricewaterhouseCoopers' Economic Crime Survey. Our fourth biennial economic crime survey provides unparalleled analysis and insight into perceptions, awareness and the impact of economic crime on businesses in India.

For long, India has been infamous for frauds such as corruption and bribery. These, along with factors like red-tape and poor infrastructure, have played a significant role in deterring multi-national corporations from investing in India during a large part of the 1980s and 1990s.

However, a lot has changed since then and India is undergoing a rapid transformation. On one hand, overseas investments into India are booming and on the other hand, an increasing number of companies are entering the global marketplace by acquiring companies abroad and by tapping global capital markets through an overseas listing. Almost every industry sector – information technology, retail, telecom, financial services, real estate, consumer durables, industrial products – is witnessing exponential growth.

In 2007, as per the World Investment Report of the United Nations Conference on Trade and Development (UNCTAD), India has emerged as the second most-attractive location for Foreign Direct Investment (FDI) after China.

Significantly, India is beginning to challenge the dominance of other Asian economies – Hong Kong, the Republic of Korea and Singapore – as the main recipient of FDI in developing Asia.

Against this backdrop, it is not surprising that perceptions about corruption, although improving, continue to pose a significant challenge for businesses in India.

Regulators in India are becoming increasingly active in identifying and investigating economic crime. For instance, the Competition Commission has been constituted to review anti-trust and monopolistic risk prior to large mergers and acquisitions. The Reserve Bank of India has also stepped up enforcement of anti-money laundering regulations. Similarly, the Foreign Corrupt Practices Act of the US and the adoption of Clause 49 in India have ensured that Indian companies install certain measures that would help curb economic crime.

Awareness about fraud risks is a growing phenomenon worldwide, and India is no exception. Increased cooperation between regulators in various countries has given rise to a new trend in enforcement. For example, the recently established Financial Intelligence Unit in India has joined the Egmont Group to tackle money laundering.

Despite all these positive developments, economic crime continues to be a pervasive threat. While technology is a

key enabler and has made companies more efficient, companies have become more vulnerable to fraud risks. Fraudsters are adept at using latest technology to perpetrate frauds. Companies, in turn, are facing formidable challenges in deterring 'new age' frauds.

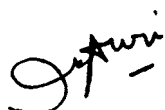
Companies in India, therefore, cannot afford to be complacent. Ignoring the potential risks of economic crime can prove costly. It can derail a company's growth plans, restrict its access to global capital markets and disqualify it from participating in projects funded by international organisations. Therefore, it is critical for companies in India to be proactive and undertake measures to prevent, detect and remediate frauds.

While fraud can never be eliminated, our experience suggests that companies that adopt a proactive and risk-based approach towards fraud risk and related controls are better equipped to combat economic crime.

We express our gratitude to corporate executives from the 150-odd companies in India who shared their views about the impact of economic crime in their respective industry sectors. We hope you will find these insights useful and relevant in your ongoing fight against economic crime.



**Steven Skalak**  
Global & US Investigations Leader  
New York, USA



**Ashwani Puri**  
Leader India Advisory Service  
& Investigations and Forensic Services  
New Delhi, India

## Economic crime continues to be a pervasive threat

Economic crime remains an intractable problem for companies globally and India is no exception. As India Inc. goes global, economic crime is emerging as a bigger threat than before. When companies in India expand their reach to other countries, they are exposed to not just 'home-grown' frauds, but also frauds prevalent in other markets.

The following key findings of the survey highlight the fact that economic crime is a serious and growing threat in India

**a. Growing mismatch between reported instances of fraud and perception of fraud:** There has been a dramatic drop in the percentage of companies that reported to be victims of fraud. However, in most categories of fraud, the respondents' perception of fraud was substantially higher than the actual incidents reported. This mismatch may imply that incidents of fraud are going unreported.

**b. Instances of corruption and bribery are on the rise:** India has been infamous for corruption and bribery. Unfortunately, corruption and bribery is one area that reported an increase in the instance of fraud as opposed to our 2005 and 2003 surveys.

**c. The cost of managing frauds is very high:** Economic crime continues to be an expensive proposition for companies, both in terms of losses and managing costs. Companies in India reported having suffered average direct losses of US \$1.5 million (INR 6 crore) due to fraud. More importantly, the cost of managing fraud (including legal investigation, stakeholder management and public relations costs) is also very high.

**d. Fewer companies are covered against frauds:** Companies in India are more exposed to fraud losses and costs than their global counterparts. Only 34% of our survey respondents from India reported having an insurance coverage to cover losses and costs from fraud against 45% of the respondents globally and 39% in the Asia & Pacific region<sup>1</sup>.

**e. Fewer companies take action against perpetrators of fraud:** Perpetrators of fraud may have been emboldened to commit fraud in India since 36% of companies in India failed to take any action against the perpetrators as against 16% of companies globally and 21% of companies in Asia & Pacific region.

**f. Whistle-blower mechanism appears to be ineffective in India:** While the findings of our 4th biennial Global Economic Crime Survey suggest that in virtually every region of the world,

whistle-blowing mechanism is playing a role in uncovering the activities of the wrongdoers, in India, things are quite the opposite. There has been a significant decline in detection of frauds through the whistle-blower mechanism (8% as compared to 22% in 2005).

**g. More frauds today are detected by chance:** In spite of increased investment in control measures, reliance on chance has increased from 37% in 2005 to 50% in 2007. Clearly, reliance on chance or luck is no basis for a strong anti-fraud program.

**h. Lack of faith in the legal system is a matter of concern:** This year, our Global Survey asked its respondents and a group of 1500 experts about risks and challenges in seven emerging markets. An astounding 89% of the experts listed lack of faith in the legal environment and prevalence of corruption as leading matters of concern in India.

**i. Companies lost business opportunities to competitors who paid a bribe:** 34% of companies in India reported loss of a business opportunity because a competitor (most probably) paid bribe. This suggests that business relationships and success may not be entirely determined on the basis of a product or service quality, efficacy and price. The corresponding global average was 24%.

<sup>1</sup> In this survey Asia & Pacific region refers to Australia, Hong Kong/China, India, Indonesia, Japan, Malaysia, Singapore and Thailand.

## 1. Economic crime: Perception versus reality

Our 2007 economic crime study reveals that 35% of companies in India were victims of economic crime during the past two years as compared to 39% and 43% of the companies surveyed in Asia & Pacific region and globally respectively (see figure 1.1).

Interestingly, the number of reported incidents of economic crime in India has decreased from 54% in 2005 to 35% in 2007 on an overall basis. There is a marked decline in incidences of economic crime reported by companies in India over the previous survey in respect of asset misappropriation, accounting fraud and money laundering (see figure 1.2). This decline is particularly striking as compared to global and regional trends in respect of asset misappropriation and money laundering (see figure 1.3).

However, when comparisons are made with the perception of crimes, such as asset misappropriation, money laundering and IP infringement, the findings reveal that respondents perceive such frauds to be significantly more prevalent than what was reported as perceived in the 2005 survey (see figure 1.4 on next page).

Even though reported instances of most frauds have showed a considerable drop, it may be incorrect to draw an inference that economic crime in India has reduced or that companies in India have been more successful at combating fraud as opposed to their global counterparts. This is because perception of frauds, an equally important indicator that determines the actual fraud risks prevalent in a country, continues to show an upward trend.

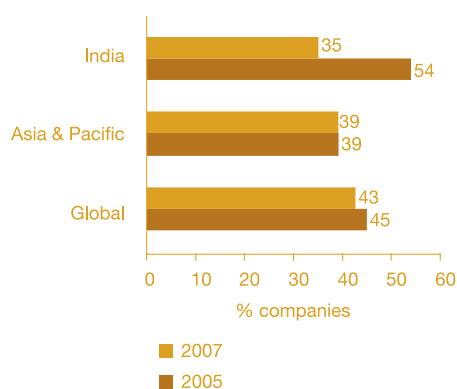
The decline in the number of reported incidents may be attributed to one or more of the following:

- Higher tolerance for fraud and a general perception that certain types of fraud are “inherent” or a necessary by-product of rapid growth
- Continued stigma attached to reporting fraud
- Reluctance to report fraud in light of increased media coverage and regulatory attention invited by scrutiny of recent corporate scandals
- Ineffective risk management systems that failed to identify fraud risks or actual incidents of fraud. Most fraud incidents continue to be discovered by chance.

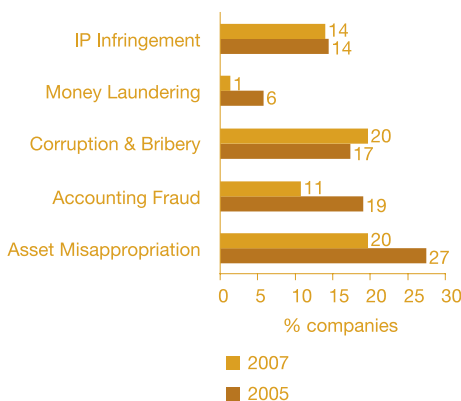
Corruption and bribery is one area in which reported fraud in India has increased since our last survey. In addition, incidence of corruption and bribery is significantly higher in India as compared to global and rest of Asia & Pacific region (see figure 1.2 and 1.3).

Our survey also indicated a significant divergence in respondents’ perception of the prevalence of money laundering and accounting fraud when compared with reported incidents (see figure 1.4 on next page).

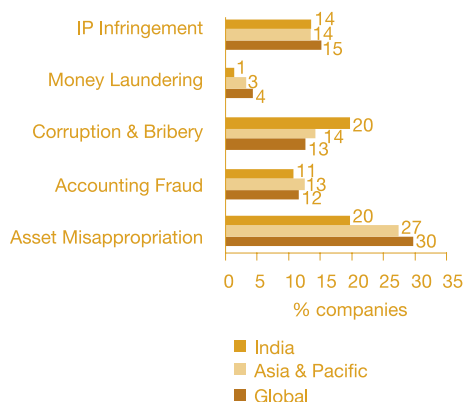
1.1 Victims of Economic Crimes



1.2 Types of Frauds-Reported Incidents



1.3 Companies reporting actual incidents of fraud



## 2. Economic crime is costly

Economic crime continues to be an expensive proposition for companies, both in terms of losses due to such crimes and the cost of managing frauds.

Companies in India suffered average direct losses of US \$1.5 million (INR 6 crore) due to fraud in the preceding two years. More importantly, the cost of managing fraud – that includes legal costs, the cost of investigating frauds, stakeholder management and public relation costs – is also very high.

Respondents in India reported average management costs of US \$1 million (INR 4 crore) – almost twice that of the global and Asia & Pacific region’s average of US \$0.55 Million (INR 2.2 crore) and US \$ 0.41 Million (INR 1.6 crore) respectively (see table 2.1), which is in addition to direct loss caused by fraud.

Quantifying losses due to frauds is quite tricky. In fact, some respondents were simply unable to put a figure to such losses. All they said was “they were significant”. It is probable that the actual losses from fraud are much higher than the reported average.

It is important to note that the reported

averages do not include the opportunity loss suffered due to counterfeit products. Nor do they consider ill-gotten revenues associated with sales contracts procured through payment of a bribe.

Companies in India are more exposed to fraud losses and costs than their global counterparts. Only 34% of our survey respondents from India had an insurance cover that would cover losses and costs from fraud against 45% of the respondents globally and 39% in the Asia & Pacific region.

As Indian companies expand globally through acquisitions and seek access to global markets through overseas listings, the importance of appropriate fidelity coverage and Directors’ and Officers’ (D&O) cover should not be overlooked.

### ‘Collateral damage’: beyond financial consequences

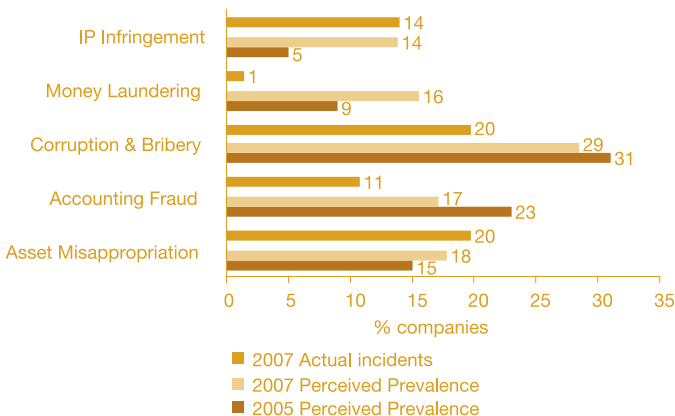
The financial damage companies suffer from fraud may only be the tip of the iceberg. The ‘collateral damage<sup>2</sup>’ from fraud can also be substantial. While quantifying financial damage from fraud is itself quite difficult, it is even harder to estimate or quantify the ‘collateral damage’.

However, damage from intangible factors such as damage to reputation or brand, decline of staff morale and impaired business relations cannot be underestimated as these elements can be undermined by the occurrence – or even the perception – of fraud.

In addition, allegations of impropriety invite unwanted attention and scrutiny from the regulatory community and can lead to severe penalties or fines. Increasingly, various regulatory agencies are jointly pursuing allegations of economic crime and are also employing latest forensic technology tools to detect such frauds.

Inevitably, substantial time and effort is expended by the management in managing public/investor relations and coordinating investigatory efforts. These distractions are likely to impact strategic business initiatives.

### 1.4 Respondents’ perception of prevalence of fraud



### 2.1 The cost of fraud

	India	Asia & Pacific	Global
Direct loss (average in US\$)	1,535,217	1,438,526	2,420,700
+ Management cost (average in US\$)	1,029,184	416,393	550,355
+ Damage to reputation or brand (% of cases)	92	89	88
+ Decline in staff morale (% of cases)	88	92	88
+ Damage to external business relations (% of cases)	84	87	84
+ Strained relation with regulator (% of cases)	75	83	80

2 Refers to intangible damage - i.e., damage to reputation of the company, brand or decline in staff morale, impaired business relations etc.

### 3. Opportunity to commit fraud is rising

It is generally accepted that frauds are committed (by individuals) when the following three conditions co-exist:

- The individual must have an incentive to commit fraud
- The individual must identify an opportunity to commit fraud
- The individual must be able to rationalise the reason for committing fraud.

Greed (64%), insufficient controls (46%) and a lack of awareness of wrongdoing by individuals (56%) were the leading reasons cited by companies when they were asked to explain why frauds were committed (see chart 3.1).

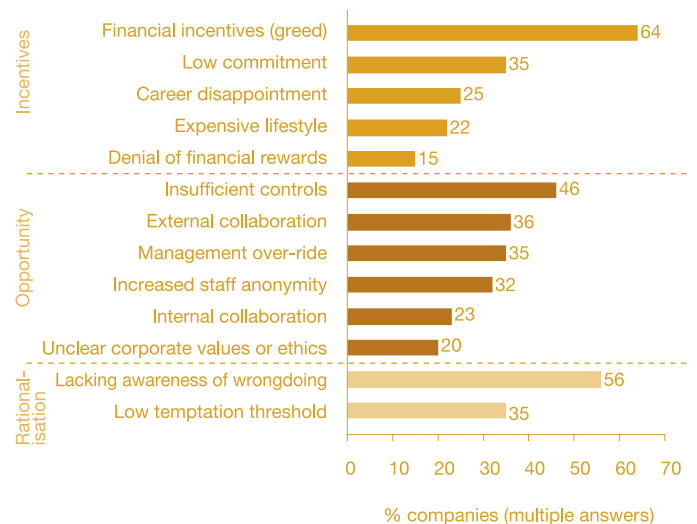
Corporate transactions, including mergers, acquisitions and joint ventures, experienced by 56% of respondents, may have created additional opportunities for perpetrators to commit fraud as companies struggled to integrate acquired entities into a uniform corporate culture.

#### The fraudster's profile

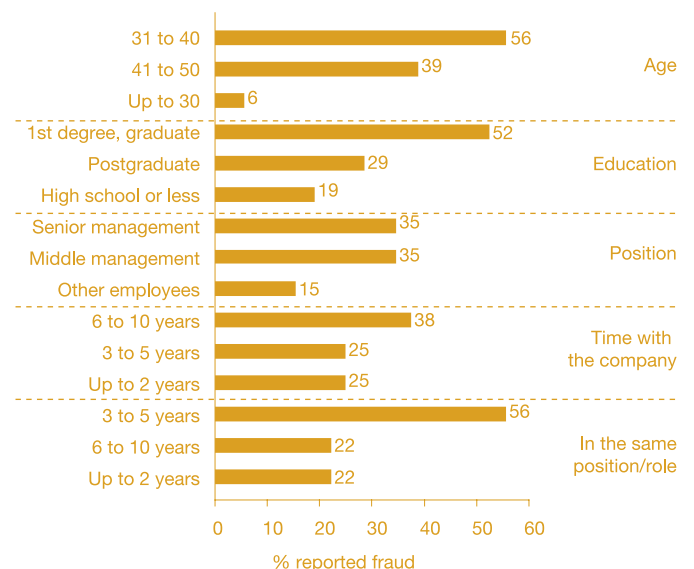
The typical perpetrator was male, between the ages of 31 to 40, with a graduate degree and was employed in the same position or role for three to five years (see figure 3.2).

The most common motives for fraud are “need” and “greed”. Opportunities for fraud arise as a result of a weak control environment in an organisation.

#### 3.1 Reasons cited by companies to explain why fraud was committed



#### 3.2 Profiling the fraudster



Individuals external to the organisation (including customers, suppliers and business partners who are related to the business as well as unrelated parties) were responsible for more than half (58%) of the reported frauds (see figure 3.3).

It is worth noting that about 31% of the frauds were committed by external perpetrators having no business relations with the company. This finding is consistent with high number of matters reported in IP Infringement such as counterfeits, software piracy and theft of IP secrets and trademarks.

The survey found that 42% of the frauds reported were perpetrated by employees. Out of these, members of senior management were responsible for 35%<sup>3</sup> of frauds. Senior management has the power to (mis)use authority and override controls that are designed to prevent or detect fraud. Therefore, frauds perpetrated by the senior management are egregious in their impact.

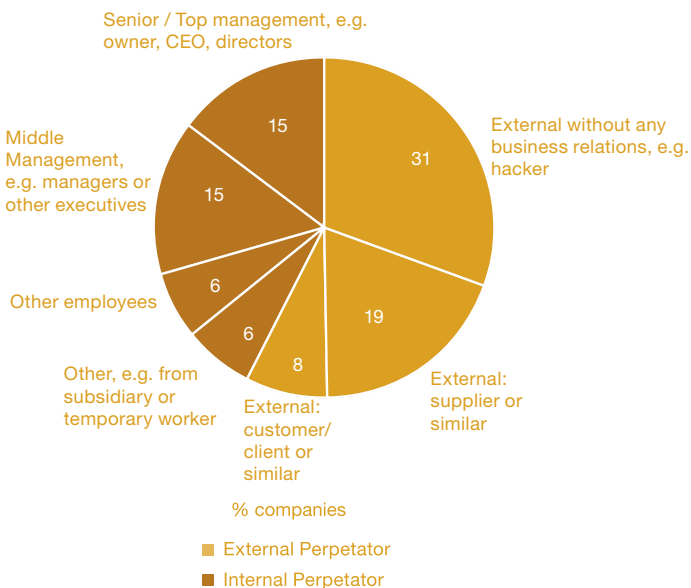
Further, perpetrators may have also been emboldened to commit fraud since 36% of companies in India failed to take any action against the perpetrators as against 16% of companies globally and 21% of

companies in the Asia & Pacific region (see figure 3.4).

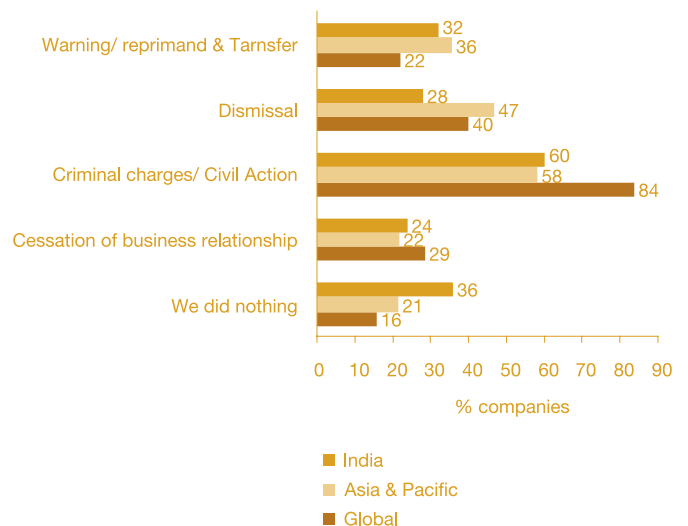
It is likely that companies in India are reluctant to initiate a long and expensive recovery process with no guarantee that the perpetrators will eventually be implicated. However, this can send a wrong message to fraudsters. Companies should send a clear message to potential perpetrators that every effort will be made to recover losses due to fraud.

**Fraudsters operating within the company understand the business and more importantly senior management can use their authority and override controls designed to prevent or detect fraud.**

### 3.3 External vs. Internal Perpetrator



### 3.4 Action taken against main perpetrator



#### 4. Internal control mechanisms designed to detect and prevent fraud have not proven to be uniformly effective

The means by which fraud is detected can be split into two broad categories

- detection through risk management controls and systems; and
- detection through chance.

##### Reliance on internal audit

In 23% of the reported cases, detection of fraud was attributed to the internal audit function, a significant increase over the 2005 survey (15%). Our experience suggests that internal audit is particularly effective in detecting fraud committed by internal perpetrators (see figure 4.1).

In contrast, detection of fraud committed by external perpetrators requires an effective risk management system, good corporate security and customised internal controls, in addition to external tip-offs (such as the whistle blower mechanism).

In virtually every region of the world, whistle-blowing is playing a role in uncovering activities of the wrongdoers (see figure 4.2).

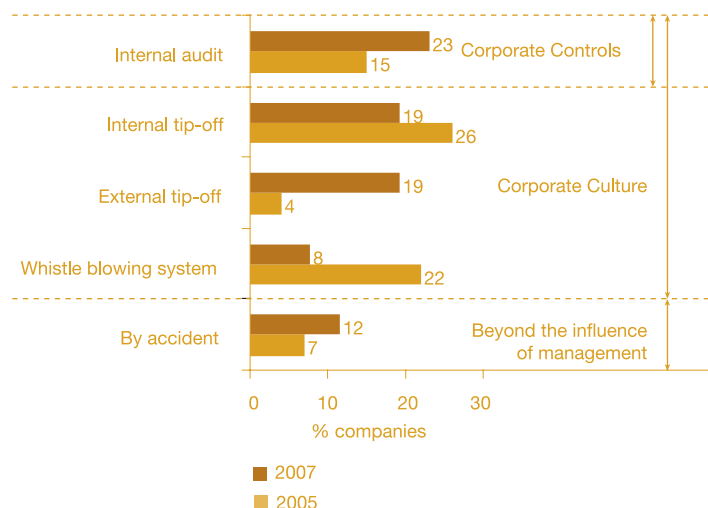
However, in India, things have been quite the contrary. There has been a significant decline in detection of frauds through whistle blower mechanism (8% as compared to 22% in 2005). This finding raises a cause for concern. Companies should appreciate that the whistle blower system works best in an environment that promotes an open culture and an ethical tone at the top – both in perception and reality. Companies in India need to work towards promoting an environment where whistle blower feel safe and believe in the system, which would encourage reporting of instances of fraud or suspicion thereof.

Fraud committed by external perpetrators who do not have any business relations with the company (e.g., cyber crime and IP infringement) are particularly difficult to detect. With increased dependence on technology, organisations need to manage such risks more effectively.

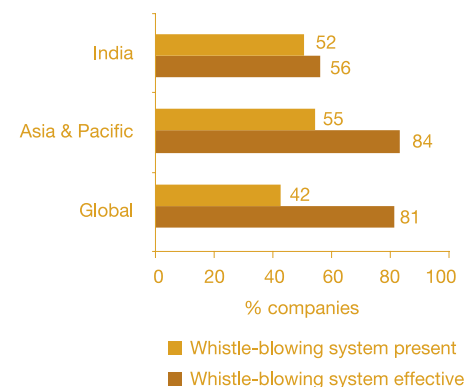
Companies are advised to assess their vulnerability and install electronic surveillance programs that can monitor and detect intrusions.

Once the fraud was detected, the internal audit function was used to investigate fraud in 65% of cases. The internal audit function is generally ineffective in probing fraud since the primary role of internal audit is to provide assurance to the management and the audit committee that internal controls are effective and working as intended. Although internal audit would seek to detect errors or improprieties during the course of its audit, such work is undertaken without any specific information on whether such improprieties exist within the Company or not. Here, a forensic accounting investigation is clearly useful. A forensic accounting investigator seeks to discover the full methods and extent of improprieties that are suspected or known.

#### 4.1 Fraud detection methods



#### 4.2 Companies that report operating a whistle-blowing system and the percentage of those that consider it to be effective



**Reliance on chance**

Even though the companies surveyed had instituted various control measures to prevent and detect fraud, fraud was detected by chance (tip-offs and accident) in 50%<sup>4</sup> of the cases. This finding too is a cause for concern.

In spite of increased investment in control measures, reliance on chance has increased from 37% in 2005 to 50% in 2007. Clearly, reliance on chance or luck is no basis for a strong anti-fraud program.

Companies have traditionally instituted controls as a reactive measure, rather than a proactive one. These measures have typically been in response to either a legislative diktat – such as Clause 49 or Sarbanes-Oxley Act – or after a rise in reported incidents of frauds.

Further, it is likely that some control elements were not understood or

implemented properly, thereby rendering them ineffective. For example, a corporate code of conduct/ethical guidelines and whistle-blower hotline were considered effective in only 63% and 56% of cases respectively (see figure 4.3).

Companies need to be more proactive in assessing fraud risks and must implement tailored controls to reduce reliance on chance.

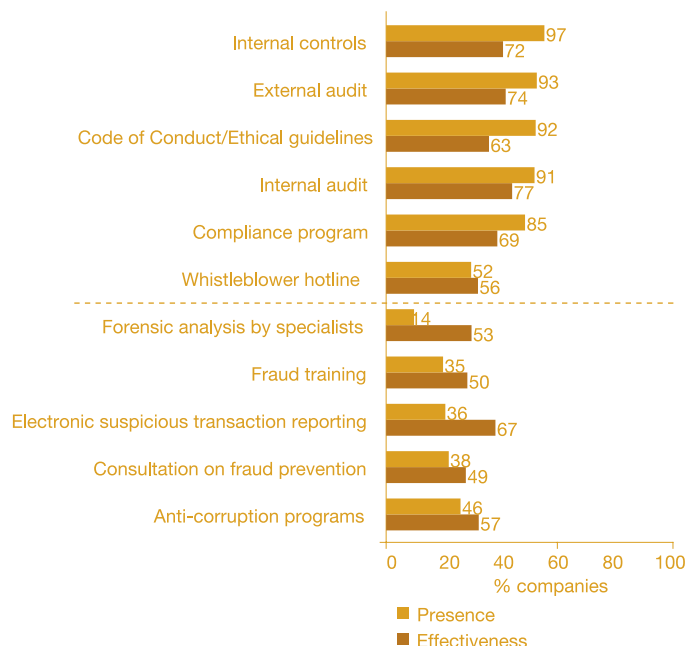
Companies should comprehensively assess fraud risks on a periodic basis in order to identify potential fraud types and to determine the likelihood of and risk of occurrence of such fraud. In addition, companies should also implement tailored controls to reduce the likelihood and impact of identified risks.

PricewaterhouseCoopers’ seven step approach to an effective fraud risk assessment covers the following:

- Organise the assessment – identify key business functions
- Determine the scope of the assessment – areas such as sales, procurement, finance and key business units should be considered
- Identify potential fraud schemes and scenarios that are inherent to the geographic region and industry sectors in which the company operates
- Assess likelihood of occurrence and impact
- Evaluate design and test effectiveness of controls
- Identify and assess residual risks
- Adjust design and implementation of controls to reflect changes in company structure and business conditions.

**50% of the cases of economic crime were detected by chance. Clearly, reliance on chance or luck is no basis for a strong anti-fraud program.**

**4.3 Presence v. effectiveness of controls**



<sup>4</sup> Internal tip-off 19% + external tip-off 19% + other accidental means 12% = 50%

## 5. Perceptions of corruption, although improving, continues to be an area of significant challenge

Recent legislative measures such as the Right to Information Act and increased scrutiny by the media have had a positive effect in lowering the perceived prevalence of corruption. Transparency International's 2007 Corruption Perceptions Index ranked India's integrity score at 3.5, slightly higher than 3.3 in 2006. However, India still has a long way to go in order to attain the 'best in class' status.

This year, our Global Survey also asked its respondents and a group of experts<sup>5</sup> about risks and challenges in seven emerging markets – Brazil, China, India,

Indonesia, Mexico, Russia and Turkey (a group which PwC terms the E7 markets). Here we combined the experiences of more than 1,500 E7 experts who contributed to our research program (i.e., senior executives with responsibility for, and experience of, investing in these markets) with our own experiences of helping companies identify and control fraud threats worldwide to offer a unique perspective on this issue.

An astounding 89% of the experts listed lack of faith in the legal environment and corruption as leading matters of concern in India (see figure 5.1).

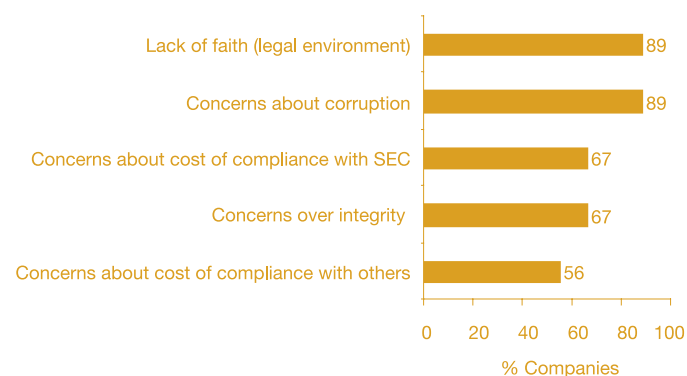
The perceived prevalence of fraud is amply demonstrated in lost business contracts and opportunities attributed to a competitor who may have paid a bribe (see figure 5.2).

It is worth noting that bribes can take many forms including monetary payments, gifts, donations, lavish travel and entertainment expenditures and sponsorships.

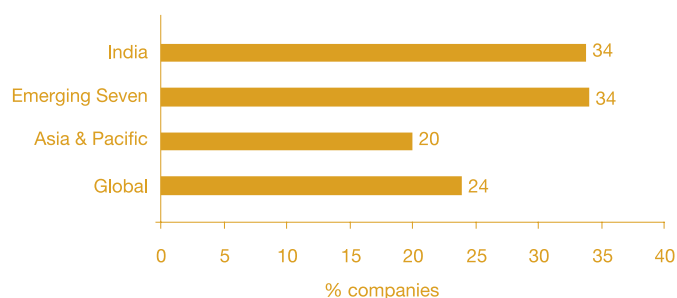
An alarming 34% of companies in India reported loss of a business opportunity due to the likely payment of bribe by a competitor, suggesting that business relationships and success may not be determined only on the basis of a product or service quality, efficacy and price. The global average is 24 per cent.

Arguably, companies in India may feel that they have lost out by not being corrupt. Should companies then consider turning a blind eye to instances of corruption in order to partake in this current period of economic growth?

### 5.1 Experts' concerns about fraud issues in India



### 5.2 Companies that lost an opportunity to a competitor who may have paid a bribe



<sup>5</sup> More than 1,500 self-accredited experts shared their perceptions and experiences in the E7 markets. The experts include senior executives with responsibility for, and experience of, investing in the E7 markets.

The answer is a clear 'no', because the threat of regulatory action – both by regulators in India and overseas – and the subsequent penalties and fines can be crippling.

Companies in India that are listed on the US stock exchanges have to contend with the US Foreign Corrupt Practices Act that requires them to accurately record their transactions and imposes severe sanctions, fines and penalties for potential violations. PwC reviewed FCPA settlements over a three-year period and determined the average settlement amount to be US \$13.5 million (INR 54 crore).

Clearly, given the substantial risks associated with bribery, companies are well advised to be forewarned about these risks rather than being caught blind sighted.

At a minimum, companies should undertake the following:

- Establish an appropriate anti-corruption compliance program, including policies for gifts and hospitality
- Conduct a training program for employees that goes beyond 'dos and don'ts' and appropriately addresses prevailing customs and practices
- Determine appropriate limits for gifts, hospitality and entertainment
- Perform a comprehensive assessment of sales agents, resellers, consultants and similar customer-facing intermediaries
- Undertake rigorous due diligence of sales intermediaries.

**34% of companies in India reported loss of a business opportunity due to the likely payment of bribe by a competitor, suggesting that business relationships and success may not be determined only on the basis of a product or service quality, efficacy and price**

## 6. The future of economic crime

Fraud has and will remain an intractable problem. While some types of fraud like asset misappropriation have remained static, others like hacking and theft of intellectual property are on the rise.

As companies in India expand their reach and presence in other countries, they are not only at the risk of 'home-grown' frauds, but also exposed to bribery and corruption risks in those markets. Additionally, safeguarding intellectual property and protecting trade secrets is paramount as competitors attempt to 'copy' or 'steal' successful products and services. Against this backdrop, detection of economic crime by chance is clearly inadequate.

Companies in India are acutely aware of these risks and 23% of the companies identified IP infringement as the leading cause of economic crime in the next two years (see figure 6.1).

It is interesting to note that perception of vulnerability to corruption and bribery, accounting fraud and asset misappropriation over the next two years are significantly lower than the current

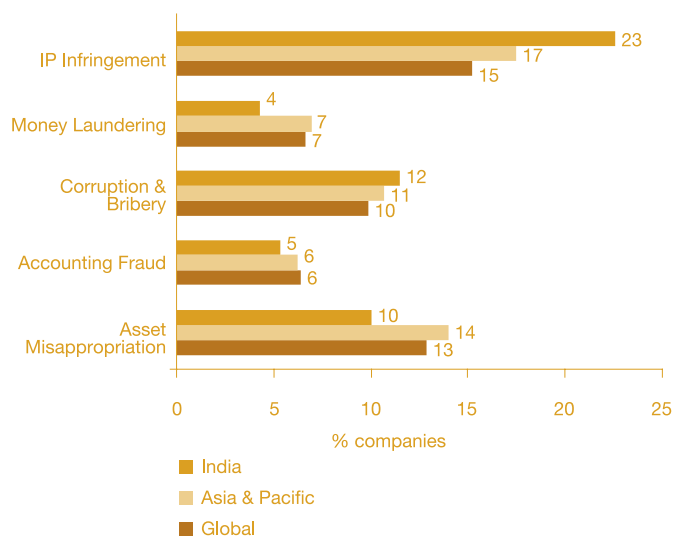
perception and actual incidence of such fraud reported by the respondents during the last two years (see figure 6.2).

Although companies have instituted several control measures to detect and deter fraud, they cannot afford to be complacent.

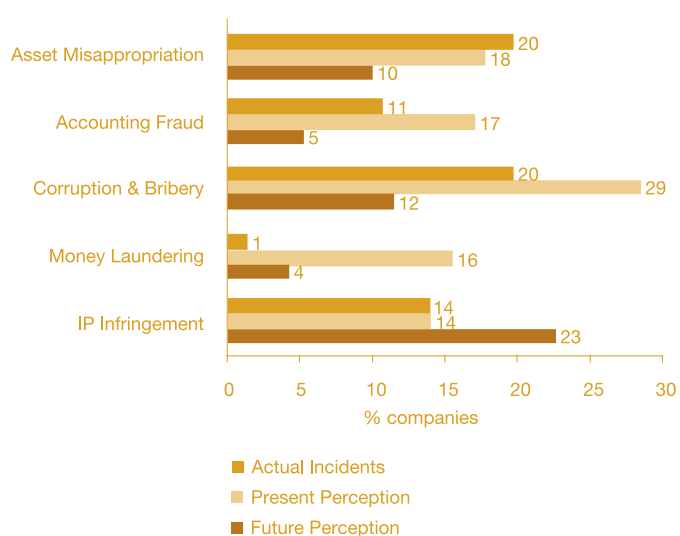
The results of our survey have clearly shown that internal control mechanisms by themselves were ineffective in preventing and detecting fraud, despite the fact that multiple controls had been installed by the companies surveyed. Instead, our experience suggests that companies that adopt a proactive and risk-based approach are better equipped to combat economic crime. This entails effectively implemented and regularly updated controls along with a strong culture of the organisation that supports a holistic compliance program working in tandem with a clearly understood code of ethics, emanating from the top management.

Fraud can never be eliminated. However, companies can endeavour to better understand fraud risks, develop and implement tailored controls and mitigate the risk of economic crime.

### 6.1 The future of economic crime



### 6.2 Present Perception vs Future Expectation



## 7. Methodology

PwC's 4th biennial Global Economic Crime Survey was conducted in 40 countries between April and July 2007 and covered over 5,400 respondents globally.

PwC retained the internationally-renowned market and social research institute, TNS Emnid, to conduct one-on-one telephone interviews in 40 countries and 21 languages. This was then followed by several weeks of careful data analysis by the independent Economy & Crime Research Center at Martin-Luther-University, Halle-Wittenberg.

The India survey is a result of interviews with 152 respondents including Chief Executive Officers, Chief Financial Officers, Risk Heads, Internal Auditors, Legal Counsel, Human Resources Directors, Compliance Officers and other functional Officers.

The survey was undertaken through computer-assisted interviews (Telephonic & Web) from a randomly selected sample of organisations in the country. Further information on survey methodology and definitions of economic crimes can be found in the Global Economic Crime Survey 2007 report and at [www.pwc.com/crimesurvey](http://www.pwc.com/crimesurvey).

<b>Industry Group Participating</b>	
	% companies in India
Industrial Manufacturing	28
Financial Services	11
Technology	11
Entertainment, Media & Communication	11
Others Industry Sectors	9
Energy, Utilities & Mining	8
Engineering & Construction	7
Automotive	6
Chemical	4
Healthcare & Pharmaceuticals	4
Transportation & Logistics	4

<b>Function (Main Responsibility) of interviewee in the company</b>	
	% companies in India
Finance	59
Audit	10
Legal	14
Human	11
Security	8
Risk	10
Compliance	15
Other function	42

<b>Size of the participating organisations</b>	
No. of employees	% companies in India
Less than 200	25
201 - 1,000	34
1,001 - 5,000	28
More than 5,000	11

## Contacts

### Investigations and Forensic Services

Ashwani Puri, Leader  
Tel: +91 124 4620 501  
e-mail: ashwani.puri@in.pwc.com

Sumit Makhija  
Tel: +91 124 4620 556  
e-mail: sumit.makhija@in.pwc.com

Vidya Rajarao  
Tel: +91 22 6669 1302  
e-mail: vidya.rajarao@in.pwc.com

N. V. Sivakumar  
Telephone : +91 80 25585663  
e-mail: n.v.sivakumar@in.pwc.com

### Forensic Technology Services

Rajarshi Sengupta  
Tel: +91 33 2357 3391  
e-mail: rajarshi.sengupta@in.pwc.com

### Business Risk

Satyavati Berera  
Tel: +91 124 4620 507  
e-mail: satyavati.berera@in.pwc.com

Tapan Ray  
Tel: +91 22 6669 1204  
e-mail: tapan.ray@in.pwc.com

Neeraj Gupta  
Tel: +91 124 4620 571  
e-mail: neeraj2.gupta@in.pwc.com

### IT Security Risk

Sivarama Krishnan  
Tel: +91 22 6669 1350  
e-mail: sivarama.krishnan@in.pwc.com

©2007 PricewaterhouseCoopers. All rights reserved. "PricewaterhouseCoopers", a registered trademark, refers to PricewaterhouseCoopers Private Limited (a limited company in India) or, as the context requires, other member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers, its members, employees and agents accept no liability, and disclaim all responsibility, for the consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

Design: info@mindcube.com Printed by: Paramount Printographics

