

Investigations and Forensic Services

# Economic crime: people, culture and controls

The 4th biennial Global Economic Crime Survey



MARTIN-LUTHER-UNIVERSITY  
ECONOMY & CRIME RESEARCH CENTER  
Prof. Dr. Kai-D. Bussmann

PRICEWATERHOUSECOOPERS 



# Introduction

We are pleased to present PricewaterhouseCoopers' 2007 Global Economic Crime Survey, the largest study of its kind now available worldwide. Based on months of interviews conducted with over 5,400 companies in 40 countries, our survey offers an in-depth look at the root causes of economic crime and the ways in which it affects businesses worldwide.

The study applies a combination of the following four research strategies:

1. **Company survey.** This survey delivers findings in which executives from thousands of companies around the world report their experiences in their own fight against economic crime. In this sense, it is currently the largest international company survey of economic crime worldwide.
2. **Case study.** Unlike other surveys, it includes case studies in which victimised companies provide detailed information on real-life crime incidents. With this approach, we can deliver more precise offender profiles, analyses of collateral damage and information on the concrete causes of crime as well as the range of company remedial actions and criminal prosecutions.
3. **Emerging market focus.** Our survey gives in-depth insights into the problems facing companies that do business in emerging markets. We gathered valuable information from more than 1,200 interviews with company managers

responsible for investment decisions in the so-called emerging seven countries (E7). This survey also contains detailed experience reports from over 500 companies on doing business in China.

4. **Eight-year trends.** The 2007 Survey is the fourth multinational survey conducted by PwC on the topic of economic crime. Our data now stretches over an eight-year period. Despite the introduction of a number of new topics, the survey remains based on a relatively unchanged core group of set questions. This enables us to plot long-term developments and experiences in the fight against economic crime and to discern key trends.

We have divided our survey into three sections. The first section ('The statistics') focuses on statistical trends and findings related to types of fraud, fraud's victims, perceptions, perpetrators and costs. The second section ('The issues') provides insights into the complex interrelationship between internal controls and corporate culture. The survey's third section ('The emerging markets') focuses on the sources, perceptions and experience of experts who are confronting the risk of fraud in some of the fastest growing economies in the world.

Our survey reveals that fraud remains one of the most problematic issues for business worldwide. Despite the attention of regulators and companies' investment

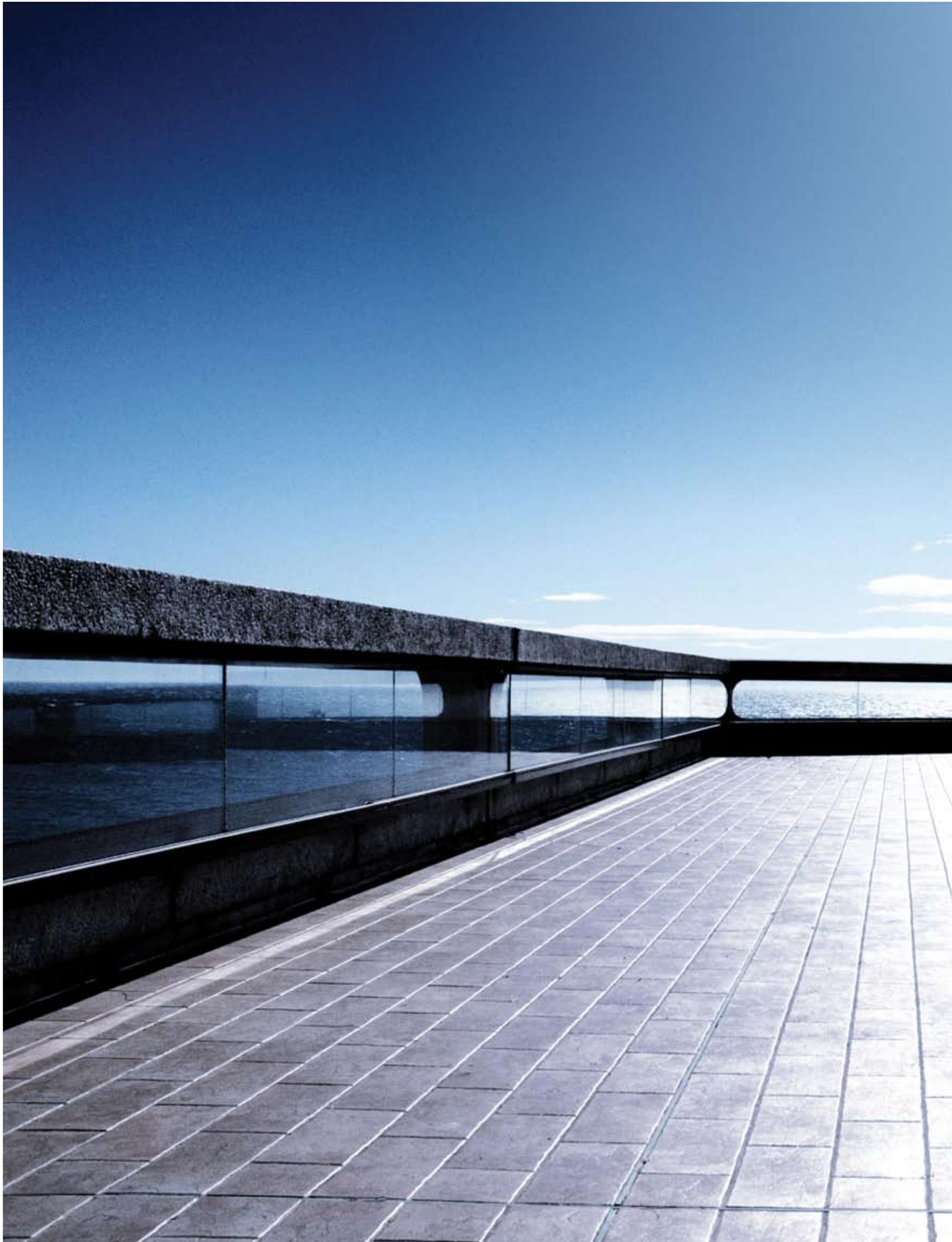
in controls, the actual level of economic crime and the associated financial and non-financial damages have not decreased – one out of every two companies fell victim to economic crime in the last two years. While companies continue to develop systems and controls both to detect and to deter economic crime, fraud controls alone are not enough. An ethical corporate culture plays an equally important role in deterring fraud. These findings are presented in the context of both developed and emerging markets – where opportunities for growth present some of the greatest challenges in detecting and deterring fraud.

As our survey clearly shows, it is simply impossible to get rid of economic crime – the crime of fraud remains intractable because of the many kinds of fraud and the correspondingly broad range of fraudsters who commit them. There will never be a simple solution, but we can endeavour to develop our understanding and share our knowledge of 'what works and what doesn't' in combatting fraud. In continuing this process, we appreciate the ongoing cooperation of the global business community, which – as in the case of this report – was willing to talk about this sensitive topic. For that, we are sincerely grateful.



# Contents

Section 1: The statistics	3
Section 2: The issues	17
Section 3: The emerging markets	27
Methodologies and acknowledgements	39



# Section 1: The statistics

Statistical trends and findings on types of fraud, victims, perceptions, perpetrators and costs



## Fraud – a most problematic business risk

Our 2007 survey reveals that fraud remains one of the most problematic issues for businesses worldwide, with no abatement no matter what a company’s country of operation, industry sector or size. Of the 5,428 companies in 40 countries that took part in our research project<sup>1</sup>, over 43% reported suffering one or more significant<sup>2</sup> economic crimes during the previous two years – an essentially static level compared with 2005 and an increase of six percentage points over 2003<sup>3</sup> (see figure 1.1).

Considering the significant investment many companies have made in fraud controls over the previous two years, why is it that levels of economic crime seem only to have stabilised in that time rather than shown a dramatic decrease?

This may, in part, be due to a ‘fraud controls paradox’: the notion that when controls are implemented in an organisation, the number of frauds detected increases almost immediately. However, their deterrent effect takes time to become visible. Potential fraudsters need to see that there is

a greater likelihood of detection and that those in breach of a company’s ethical, regulatory and legal guidelines will be consistently subject to sanctions that fit the offence.<sup>4</sup>

There may be other explanations for these consistently high figures. Certainly, over recent years there has been an increase in corporate transparency and a greater willingness by companies to admit that frauds have been uncovered, but we also experience a feeling among some executives that the ‘self-report and remediate’ programme encouraged by many regulators may subject them to a high and unfair cost burden relative to companies that take an alternative approach to dealing with fraud.

And the threat remains problematic, no matter the size of the company. While larger firms will inevitably suffer a greater number of frauds, the proportional difference may be due to a number of factors, including greater levels of anonymity and devolved responsibilities among staff, as well as more complex and interconnecting processes and systems leaving potential ‘control gaps’ for fraudsters to exploit (see figure 1.2).

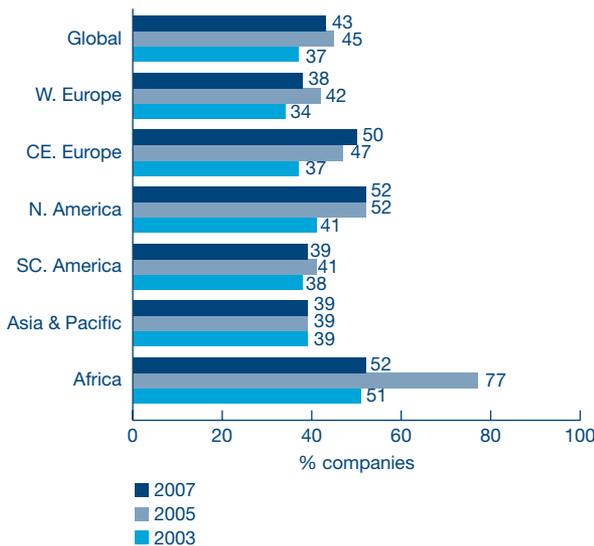
We are, of course, conscious that in collecting this information we are reliant upon our respondents’ opinions and willingness to disclose information. As a result, these figures must stand as a minimum percentage of companies that have suffered significant fraud in the previous two years: the actual figure may be much higher.

## The changing awareness of fraud

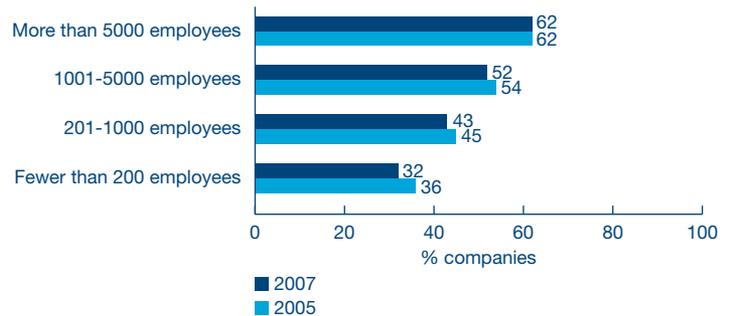
In each of our surveys, we have offered a comparison of the views held by executives regarding which types of fraud they think are prevalent and those which they have actually suffered. With four surveys of data now in hand, we are able to compare how opinions have changed over the last eight years (see figure 1.3).

Our respondents perceive that of all the fraud risks we assessed, asset misappropriation is the only one to have become consistently less of a threat, while the threat from accounting fraud, money laundering, intellectual property (‘IP’) infringement and corruption and bribery (at least since the last survey) has increased.

### 1.1 Companies reporting fraud (2003-2007)



### 1.2 Companies reporting fraud, according to their number of employees



1 The 2007 Crime Survey is the fourth multinational survey conducted by PricewaterhouseCoopers and our data stretches over eight years.

2 The term ‘significant’ was left to the discretion of the individual respondent with the proviso that it should relate to economic crimes that had a definite impact on the business, whether direct tangible damage or collateral and psychological damage.

3 Copies of our previous global economic crime surveys can be found at [www.pwc.com/crimesurvey](http://www.pwc.com/crimesurvey)

4 For further details, see Section 2, page 22.

The ebbs and flows of this ‘perception index’ are often driven by many factors, from an increase in global business activity to an increase in the awareness of fraud in general and of certain frauds specifically. And, of course, there is the noise created by media interest in a particular crime (especially when a company has fallen foul of it), or by regulatory or legislative guidelines promulgated by national governments or trans-national bodies like the Organisation for Economic Cooperation and Development (‘OECD’). With both governments and trans-national organisations focused on combatting corruption and money laundering over the past few years – as well as there being some high profile newspaper coverage of infractions by multinational companies – it is not surprising that the awareness of these types of fraud has grown.<sup>5</sup>

But why do accounting fraud and corruption and bribery have such consistently and comparatively high perceived threat levels? In our opinion, the perception levels are greater than the actual levels of fraud when the potential impact of the risk is known to be large. And the inverse is true when the potential impact is small. For example, for

**Corruption – perceptions truer than reality?**

In the case of corruption and bribery, further analysis reveals that respondents’ perceptions of the risks of this particular economic crime in their home countries were very similar to the worldwide findings reported in Transparency International’s Corruption Perception Index of 2006 (CPI). This may be because many managers, while being reluctant to report on corruption in their own company, are quite able to provide a realistic estimate of their national risks. Furthermore, their opinions of corruption are influenced by definitions that employ neutral terms and many still regard this particular economic crime as one that is peculiar to public sector organisations and government. It is possible – even probable – that companies’ perceptions generally appear to be more valid than the low actual incidence rates for corruption and bribery reported.<sup>6</sup>

listed companies the impact of the theft of 100 crates of inventory is considerably less than the impact from deliberately misstated financial accounts and the damage this

causes to brand, share price and business relations, not to mention the costs involved in appropriate regulatory investigations and remediation.

In addition, the volume of business transacted in the emerging markets along with an acute awareness of the lack of IP protection may be a reason for the doubling of the perception of IP infringement as a fraud risk, since there are now many well-documented cases of companies finding counterfeits of their own goods, and significant examples of grey market trading.

So how do our respondents’ perceptions compare with the actual incidents of fraud that companies have experienced over the last two years (see figure 1.5)?

Since the deployment of many controls that were reported in our 2003 study, actual incidents of asset misappropriation and accounting fraud have remained broadly static between 2005 and 2007. There has been marginal growth in the number of cases of corruption and bribery being reported although, significantly, there has been an increase in the number of money laundering and IP infringement cases.

**1.3 Respondents’ perceptions of the prevalence of fraud in their industry, in their country (2003-2007)**



**1.4 Companies reporting suffering actual incidents of fraud (2003-2007)**



<sup>5</sup> For overview, see, Johann Graf v. Lamsdorf, The Institutional Economics of Corruption and Reform, 2007.

<sup>6</sup> According to the CPI, for instance many Asian countries reveal even higher rates than are shown by our results. Kai D. Bussmann, Markus Werle, ‘Addressing Crime in Companies’, British Journal of Criminology, October 2006, p.1128ff.

While money laundering is largely restricted to the financial markets, the high number of cases has particularly affected organisations in North America (8% of companies). This may not be surprising because of its importance in the world capital markets. Cases of IP infringement have been prominent in Central and Eastern Europe (20% of companies). This increase in reporting may in part be due to membership of the European Union and its influence on corporate transparency. However, in North America (19%), this may be due to companies' IP being stolen by fraudsters overseas. Reports of corruption are more widespread in Central and Eastern Europe (18%), South and Central America (11%), Africa (28%) and Asia and Pacific (14%).

The continued high level of reported frauds and the continuing high perception levels of the risks might lead to the conclusion that the controls designed to detect and prevent fraud have not proven to be uniformly effective. However, to date, many of the controls that companies have implemented are focused on procedures to deliver accurate financial reporting. The new and

updated controls often do not explore other areas of potential fraud risk, such as asset misappropriation or corruption and bribery, for which specific fraud risk management controls and activities are needed. Even for organisations that have established controls in these areas, one must consider the inherent delayed deterrent effect of such controls. Both the previously mentioned 'fraud controls paradox' and, most importantly, the fact that fraudsters will always try to find ways to circumvent even the most rigorous of controls impact the perceived current effectiveness of controls. Hence it is our proposition that the value of controls lies in ensuring that:

1. Controls are continually upgraded and adapted to thwart the fraudster;
2. Controls reflect the culture of the firm and its ethical guidelines (which incorporate the explicit norms of criminal law); and,
3. Any cases of fraud that are detected trigger an immediate, appropriate and consistent punitive response, no matter what the position of the perpetrator inside or outside the firm.

#### Assessing your perceptions of fraud with the threats you face

Deceit is the hallmark of economic crime – it remains hidden within the practices and processes of a business. So it is natural to decide upon and invest in controls to deal with the fraud risks that you perceive to be a threat to your business. But the question remains whether that investment is properly focused in order to render it effective? After all, as you can see in figure 1.5, perceptions of risk can differ from the actual levels of threat.

Before establishing further controls, seek professional advice to confirm whether your perceived threats weigh-up against the actual risks you face and use that information to make decisions on the controls that you need and the costs of implementing them.

But remember, while controls and procedures can help limit or prevent losses from asset misappropriation or other economic crimes, it is the implementation of an effective culture of compliance within your organisation that will help prevent a catastrophic monetary loss or a business failure from economic crime.

#### 1.5 Perceived prevalence vs companies reporting actual incidents of fraud



controls designed to detect and prevent fraud have not proven to be uniformly effective

## Fraud's impact on industry

Yet again, our research shows that no industry is immune from the threat posed by economic crime. Indeed, for three sectors, more than half the participating companies reported suffering fraud during the previous two years. The idiosyncrasies of each of these sectors will be explored in more detail in our industry-specific supplements. However, it is of value to draw attention to some of the highlighted statistics here, particularly in relation to sectors' perceptions as to the prevalence of fraud (see figure 1.7).

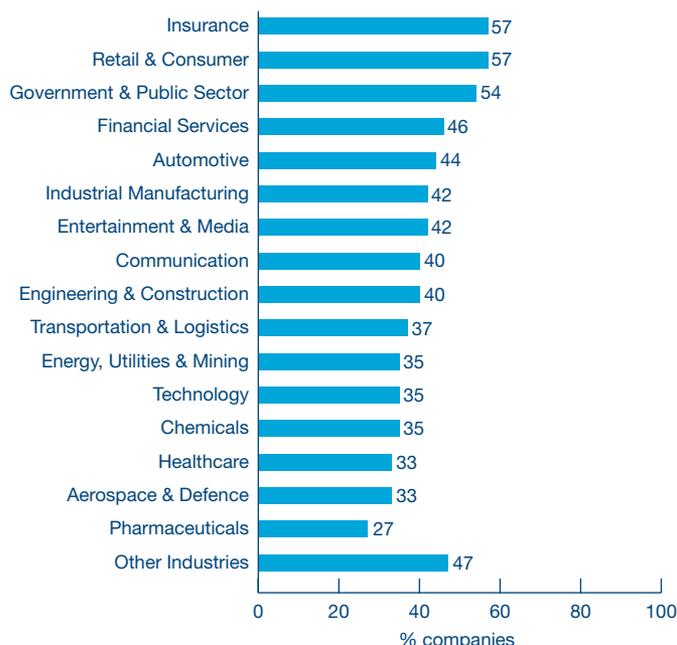
For many, it may be no surprise that the financial services have not only the highest perception of the prevalence of money laundering in their sector (16% of companies) but that they also suffered the most from it, with 17% of companies reporting this particular economic crime. Similarly, the technology sector indicated the highest perceived prevalence of IP infringement (20% of companies), and 19% of the technology companies also reported being victims from it.

However, while 24% of retail and consumer companies believed that asset misappropriation was most prevalent in their sector, it was in fact the insurance sector where the most companies reported suffering this fraud (46% of companies). And while 25% of engineering and construction companies perceived corruption and bribery to be most prevalent in their sector, it was again the insurance sector that reported the most companies falling victim to it (19% of companies) (see figure 1.7).

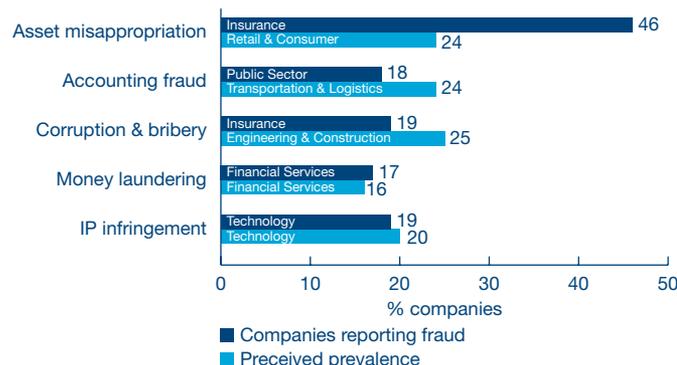
The insurance sector also reported the greatest direct losses from fraud: on average, it reported a loss over two years of US\$ 4,476,717, and spent, again on average, an additional US\$ 1,018,114 on managing the issues resulting from it. In fact, seven sectors reported higher than average losses over the course of two years, some of them considerably higher. The impact of these costs will be explored in the next section.

	Average direct loss (US\$)	Average management cost (US\$)	Total average cost to business (US\$)
Global	2,420,700	550,356	2,971,056
Insurance	4,476,717	1,018,114	5,494,831
Industrial Manufacturing	4,337,975	758,851	5,096,826
Technology	3,462,819	554,895	4,017,714
Entertainment & Media	3,118,516	300,862	3,419,378
Engineering & Construction	2,919,975	360,313	3,280,288
Retail & Consumer	2,605,749	481,224	3,086,973
Pharmaceuticals	2,479,047	357,251	2,836,298

### 1.6 Companies reporting fraud by industry sector



### 1.7 Sectors that perceive frauds as most prevalent compared with those with the most companies reporting it



## The cost of fraud

The immediate response of most executives to an instance of fraud is, 'How much has this cost us?' Typically, this concern is directed towards the actual monies stolen, and our study shows that these are substantial.

Average loss from fraud over two years per company in 2007: **US\$ 2,420,700**  
Average loss from fraud over two years per company in 2005: **US\$ 1,732,253**

In some cases, this is an estimated cost and, in our experience, most likely an undervaluation. In particular, if one considers the amount of undetected losses of companies with a weaker control environment, our study reveals a significant increase in the average of the total financial losses to **US\$ 3,242,095** (on average worldwide per company).<sup>7</sup>

One must also bear in mind that there are many cases where the respondents to our research were simply unable to put a figure on their losses except to say 'they were significant'.

Total loss reported by respondents over two years:  
**in excess of US\$ 4.2 billion**

Estimated total losses including the undetected losses of companies with a weaker control environment:  
**US\$ 5.7 billion**

It is also worth recalling that for certain crimes, for example in cases of money laundering, there is no immediate financial cost to the firm since it was merely a channel for attempts to legitimise the proceeds of crime. Similarly, accounting fraud may see the manipulation of company figures to disguise underperformance, but in itself may not involve any direct losses. Corruption and bribery may see the payment of cash or gifts to secure a contract or favour, but these are, in themselves, not often 'losses' to the company. And the consequences of IP infringement can only be truly assessed in terms of sales opportunities lost through counterfeit or grey market trading (see figure 1.8).

Yet, there are also 'management costs' involved in dealing with the fall-out from a significant fraud, from the reallocation of management time to the possible costs of litigation in retroactive action, and from the need to manage a possible PR campaign to

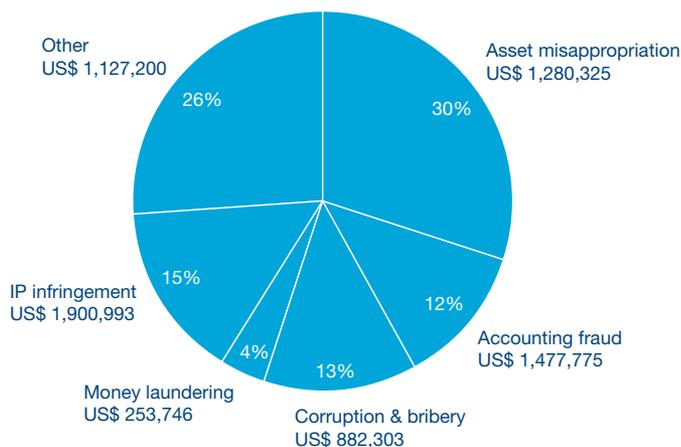
dealing with renewed regulatory oversight and demands, which our respondents who have suffered frauds have estimated at an average of **US \$550,356** over the course of two years (see figure 1.9).

If the loss of nearly US\$ 3.2 million still seems insignificant, consider the collateral damage from fraud, for it is here that one sees the potentially crippling impact of economic crime.

These are the costs that derive from 'collateral damage' to the company's brand and customer trust; to the share price and shareholder trust; to the company's relationships with its suppliers; and to staff morale, which can precipitate a loss in productivity.

The relative importance of fraud's collateral damage can be seen in the fact that over 80% of our respondents who suffered fraud also stated that this had caused damage – or significant damage – to their business (see facing page: 'What fraud costs'). While the immediate loss from fraud may have been of little direct consequence, its reputational damage and its ability to distract management from 'business as usual' were regarded as critical by our respondents.

### 1.8 Victimization rate combined with average loss by type of fraud<sup>8</sup>



### 1.9 Fraud's impact on management time and costs



<sup>7</sup> One of the most common questions we hear is, 'How did you arrive at this figure?' especially when it seems so hard to put a value on losses from fraud. Our survey explores two types of organisation: those that have up to and including five fraud risk management measures (Group A) and those that have more than five (Group B) and in a later section (see page 19) we compare the two groups' success at detecting and preventing fraud. In this instance, we used the loss figure provided by Group B companies as a reference group for estimating the undetected financial losses for the Group A companies as Group B's more advanced detection methods provide a more accurate figure for losses sustained by a company. When we compare these 'real' results with the figures estimated by companies, the average company's loss from fraud over two years increases from US\$ 2.4 million to US\$ 3.2 million – up from the figure of US\$ 1.7 million recorded in 2005.

<sup>8</sup> The costs of accounting fraud are so low because none of the respondents reported a case of false financial reporting on a public stock market: these costs relate to other losses from acts of financial misrepresentation. In addition, some companies reported 'other' crime types outside the particular frauds we were researching, including cyber crime, fencing or the handling and selling of stolen goods/products, tunnelling or the illegal sale of former state-owned goods, etc.

It is also apparent that the level of collateral damage is directly proportional to the seniority of the perpetrator: the higher the management position, the greater the trust that is bestowed, and any breach of that trust can have a dramatic impact, not only on relations with company staff, but also with clients and other stakeholders. Our research showed that there can be significant collateral damage when a member of the management team is involved. For example, on 29% of the

#### What fraud costs

Direct losses (on average)	US\$ 3,242,095
+	
Management costs (on average)	US\$ 550,356
+	
Damage to the brand	88% cases
+	
Damage to staff morale	88% cases
+	
Damage to external business relations	84% cases
+	
Costs of dealing with the regulator	84% cases
+	
Damage to relations with the regulator	80% cases
+	
Damage to share value	9% cases

#### Fraud costs: perception versus reality

Accounting fraud and corruption and bribery are two types of fraud, which, while being on average financially significant, are even more onerous when prosecuted in certain jurisdictions such as the United States. As a point of reference, PwC's 2006 Securities Litigation Study<sup>9</sup> looked at the settlements in cases involving false financial reporting by registered companies. As shown below, the average settlement cost of US\$ 66,400,000 is significantly higher than the average accounting fraud cost of US\$ 1,477,775 as reported by participants in this global survey.

2004-2006: accounting cases				
Year settled	2004	2005	2006	Average
Number of settled cases	78	84	77	
Total settlement value (excluding Cendant, Enron and Worldcom)	US\$ 2,682,400	US\$ 7,406,100	US\$ 5,708,000	
<b>Average settlement cost</b>	<b>US\$ 34,800</b>	<b>US\$ 90,300</b>	<b>US\$ 74,100</b>	<b>US\$ 66,400</b>
Settlements in thousands				

Similarly, with corruption and bribery, when prosecuted according to the laws of the United States, the fines and penalties can be significantly greater than the average cost reflected in this study. PwC reviewed FCPA settled cases over a three-year period and found the average settlement cost to be US \$13,500,000. Again, this is significantly higher than the average actual corruption and bribery cost of US\$ 882,303 as reported by participants in this survey.

2004-2006: FCPA cases				
Year settled	2005	2006	2007	Average
Number of settled cases	5	5	5	
Total settlement value	US\$ 37,200	US\$ 86,700	US\$ 78,100	
<b>Average settlement cost</b>	<b>US\$ 7,440</b>	<b>US\$ 17,340</b>	<b>US\$ 15,620</b>	<b>US\$ 13,467</b>
Settlements in thousands				

The dramatically larger and often well-publicised losses in certain jurisdictions most likely account for the fact that survey respondents perceive these types of economic crimes to be more frequent than the actual number of reported incidents.

over 80% of our respondents who suffered fraud also stated that this had caused damage – or significant damage – to their business

occasions where senior managers were involved in fraud, the collateral damage to the brand was very significant, whereas the same was true for only 7% of cases with middle managers and 5% for other grades (see figure 1.10).

The relative importance of fraud's collateral damage can be seen in the increasing number of companies that have reported it since 2005: those reporting collateral damage from asset misappropriation have increased by 66%, IP infringement by 26%, corruption and bribery by 16% and accounting fraud by 9%.

Most surprising of all is the collateral damage that accrues from money laundering, which our research shows to have more than doubled since 2005. This may be a little unfair, since the companies that have been used to channel criminal proceedings are often the victims of fraud, not the perpetrators. Yet, with the increased attention on money laundering in the fight against organised crime and terrorism, these 'victims' are often considered facilitators to the fraud since their lack of controls and processes provided the opportunity for the money laundering in the first place.

## Means of detecting fraud

We compared businesses' current effectiveness in detecting fraud with their collective performance in our previous study. And the result is continuing evidence of the intractability of fraud – and its apparent immunity to management's attempts to control it: in 2007, 41% of frauds were detected by chance, an increase of seven percentage points in the past two years.

There is a variety of possibilities to explain this disappointing reading. It may be that there has been insufficient time for companies to embed updated controls into their operations and, as a result, the controls require yet more time for their deterrent effect to penetrate the psyche of the potential fraudster. It may also be, however, that companies are investing so much in controls to guard against financial reporting risks and frauds that their eyes can be taken off other important areas of fraud risk management and compliance, such as sales practices, which may fall foul of anti-corruption laws.

Our experience from repeated research programmes shows that controls alone are not enough to take full advantage of the detection mechanisms that a pro-active

management team can create within its company. We observe, for example, the consistently high response rates from companies showing that the initial means of detection is via a whistle-blowing hotline (8% cases) or tip-off (from an internal source in 21% cases and an external source in 14%). It is our view that this results from employees being both encouraged, and facilitated, to do the right thing – which is a function of culture as opposed to control (see figure 1.11).

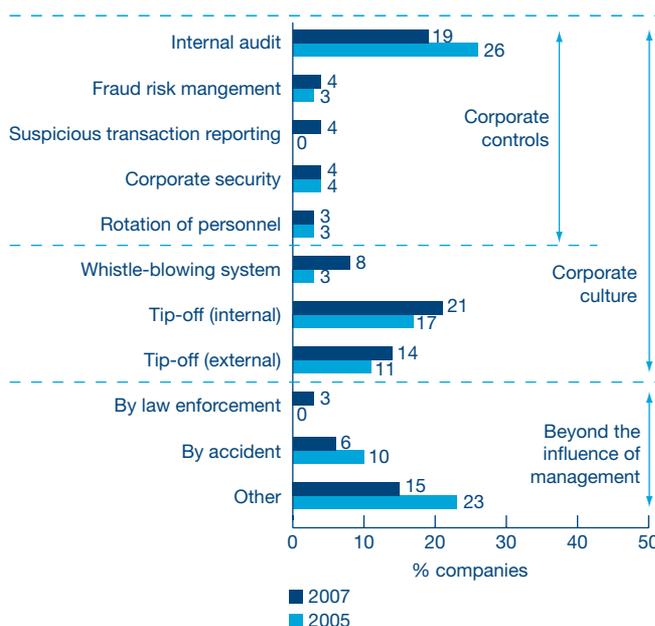
Effectively implemented whistle-blowing systems – and a corporate culture that supports them – have had a noticeable impact, detecting fraud in 8% of cases, almost three times the effect they had in 2005. Moreover, if a whistle-blowing system was rated as 'effective' by the company surveyed, it almost doubled the rate of detection (to 14%).

In certain regions, such as North America, a whistle-blowing system is now a statutory requirement of a listed company and has become a fixture of the company culture. Indeed, our study shows that management, by propagating the right ethical tone within its business and trading practices, can make a substantial impact on levels of fraud detection, in some cases reducing

### 1.10 Companies reporting significant collateral damage associated with perpetrator's position



### 1.11 Detection methods<sup>10</sup>



<sup>10</sup> New controls which were unreported in previous surveys, such as automated electronic suspicious transaction reporting systems, may account for the drop-off in the number of frauds being detected by internal audit as they are likely to detect an economic crime prior to internal audit's retrospective review.

the chance of the detection of fraud 'by accident' to as low as 20% of cases.

The value of strong fraud risk management activities at both the cultural and control level remains unquestionable. Our 2007 research once again shows the correlation

between a higher number of fraud risk management activities and a higher chance of detecting fraud, by comparing two groups: one with up to five fraud risk management controls (on average three), the other with more than five controls. It is clear to see that those with more

controls not only detected more fraud, but that they were also able to more accurately assess the associated losses.

Our research also revealed that companies in Group B had more frequently taken professional advice from law enforcement officers, lawyers or forensic accountants, to ensure that their fraud risk management tools were not only more effective and efficient, but also closed gaps between systems. A lack of such advice and of fraud awareness may lead companies like those in Group A into a cycle of deceptive security, neither knowing the risks that they face, nor being aware of their vulnerability to new types of fraud. With fewer controls, they detect fewer instances of fraud and, as a result, have less insight into the effectiveness of their existing fraud risk management measures (see figure 1.12).

**The circle of deceptive security – company performance on fraud prevention and detection**

	<b>Group A Companies with up to and including five controls</b>	<b>Group B Companies with more than five controls</b>
Percentage of companies taking professional anti-fraud advice	12%	49%
Percentage of companies that reported detecting fraud	38%	47%
Average number of frauds detected	6	10
Average loss detected for all frauds per company	US\$ 901,285	US\$ 3,419,151
Average financial costs companies spent on managing frauds	US\$ 305,227	US\$ 701,832
Insurance taken to cover losses and costs from fraud	28%	47%
Percentage of companies with significant collateral damage and associated managing costs	26%	23%

**From fraud detection to fraud prevention**

While carefully implemented and regularly updated controls can themselves be effective in detecting and, over a period of time, deterring fraudsters, our research also shows that it is the culture of a company – one that supports a holistic compliance programme working in conjunction with a

**1.12 Fraud risk management controls implemented by companies in Group A (up to five controls, and on average three) and Group B (more than five controls)**



the value of strong fraud risk management activities at both the cultural and control level remains unquestionable

clearly understood, and lived, code of ethics – that is the true foundation for an effective anti-fraud programme (see figure 1.13).

Key to this 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 appropriate to the country of operation. In our 2005 study, we suggested that, in order to limit the risk of fraud, good guidelines should ‘create a commitment to shared values... develop people’s capabilities to engage in moral reasoning and... create an environment that enables responsible conduct’.<sup>11</sup> The data from our 2007 research continues to show that this is the case.

### Internal or external fraudsters?

Of the 43% of companies that reported a significant economic crime, more than three-quarters (76%) reported that a party external to the company played a role in the fraud. And of that 76%, over a third (34%) reported that, in at least one of the reported cases, the external party was located in a foreign country.

Companies operating in the developed markets that have a high foreign trade turnover, or production and/or supplier operations in the emerging markets, typically reported a greater number of cases involving a foreign party. But, with the increasingly global marketplace, one of the most interesting statistics in our research shows that while some businesses may feel the need to act in an inappropriate manner in order to do business and compete successfully, this is not actually the case and that companies which compete while acting within their compliance guidelines actually perform better.<sup>12</sup>

When we asked respondents to comment on one or two specific instances of fraud that their company had experienced, a slightly different picture of the perpetrator’s relation to the business emerged, with half of the perpetrators being inside the company (50% internal; 50% external).

When it comes to those perpetrators who are company employees, our 2007 research results reflect our previous studies, showing a decreasing number of frauds being detected among individuals higher up the corporate ladder. This may be because the more complex economic crimes such as accounting fraud, which are harder to detect, are more likely to be

committed by senior management figures, whereas more ‘simple’ frauds such as asset misappropriation, which are often

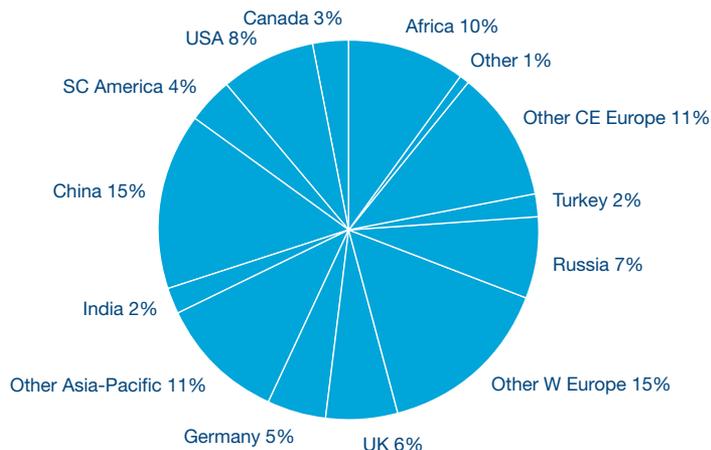
#### Influencing the behaviour of suppliers through contractual requirements, such as:

- the adoption of ethical guidelines and anti-fraud conventions from the OECD, the UN and other trans-national organisations
- access to whistle-blowing hotlines
- agreement to share an ethical code of conduct
- asking suppliers to sign statements pledging to adhere to stated guidelines
- agreeing to behavioural codes while on company premises
- requiring the pre-approval of sub-contractors or agents
- using questionnaires to gather information about sub-agents used by suppliers
- having a due diligence process for all acquisition and procurement matters
- annual re-certification of staff capabilities and processes
- internal audit rights
- external audit rights
- adoption of anti-money laundering and relevant compliance guidelines

**1.13 Companies with both ethical guidelines and compliance programmes report suffering fewer economic crimes**



**1.14 Regions from which foreign perpetrator was operating**



11 Marie McKendall, Beverly DeMarr and Catherine Jones-Rikkens, ‘Ethical compliance programmes and corporate illegality: testing the assumption of the corporate sentencing guidelines’, Journal of Business Ethics, June 2002.

12 More details about this can be found in ‘The emerging markets’ section of this report (see page 32).

easier to detect, may be perpetrated in an unsophisticated manner by staff in positions across the entire organisation.

### The driver for fraud

It is generally accepted, by criminologists and fraud investigators that three things must be present for a fraudster to set to work: the opportunity to commit fraud, the incentive to commit fraud and the fraudster's ability to rationalise their own actions.

For the purposes of this research, and for clarity in speaking with our respondents, we refined these into two areas:

- a) The perpetrator's personal reasons for committing fraud (that is, their incentive and ability to rationalise their actions to themselves)
- b) The organisational reasons that allowed fraud to occur (that is, their levels of control and the ethical culture within the firm) (see figure 1.15)

Looking more closely at our respondents' answers, we see that while insufficient company controls appear to have played a significant role in over a third of cases (34%) perpetrated, we must also take

into consideration the importance of a company's culture (and the employee's relation to it). Various other reasons cited include a low level of commitment to the firm (34%), relative anonymity (17%) and lack of clarity about the company's ethics (14%).

When a fraudster has the opportunity to operate in an environment such as this, bolstered by a self-rationalised, financial incentive (57% of cases), even the best of control systems cannot always prove effective in detecting and preventing fraud.

Company culture is therefore vital in establishing an ongoing, effective fraud risk management programme. Firstly, a clear understanding of the ethical guidelines by all staff, at every grade, is key, including the organisation's sanctioning process and its attitude of 'zero tolerance' to fraud. While many companies may have an ethical guidelines handbook, this does not always mean that its contents are well known or understood by the staff and, in our experience, many issues can arise when companies do not train their staff in appropriate corporate behaviour.

Secondly, a loyalty to the company by staff, engendered by its honest, fair and transparent actions, can serve to

encourage employees to act as its guardian, safeguarding it against those that would steal from it or damage it by their actions.

### The typical perpetrator

Our 2007 study reveals that the demographics of a typical fraudster remain unchanged from our previous research in 2005. The perpetrator is male (85% of cases) and between 31-50 years old (72% of cases). Education levels are spread across the spectrum, with half being educated up to high-school level (50%) and half having a bachelor's or postgraduate degree. Similarly, their position in the affected organisation was spread across all grades, with 52% of perpetrators falling within middle or senior management. Such high education levels and management positions should not be surprising as neither limits an individual's desire to increase their own material gain and in some cases it may help in the circumvention of sophisticated control systems. And while many new controls are able to detect the frauds committed by staff at all grades, in our experience they do not of themselves prevent the committed fraudster; in fact, as revealed earlier, it is the frauds committed by those

**1.15 Reasons cited by companies to explain why fraud was committed (multiple answer)**



company culture is vital in establishing an ongoing, effective fraud risk management programme

in the senior and middle management that cause the greatest financial and collateral damage to a business (see figure 1.16).

### Dealing with fraudsters

An important step in creating a corporate culture that does not tolerate fraud is consistency of action when economic crime is detected. When staff understand the probable personal and legal consequences of their potential foray into fraud, and that detection is likely due to the sophisticated and effective nature of the risk management systems, this serves to deter many would-be criminals.

It is interesting to note that when a fraud was perpetrated by someone outside the company, it was reported to a regulator in 38% of cases, and to law enforcement officers in 64% of cases, whereas when perpetrated by an employee, the incident was reported to regulators in only 24% of cases, and to law enforcement officers in only 55%.

Our research also shows that, around the world, the majority of significant frauds were immediately reported to senior management within the company (81%), although this is now, of course, a regulatory requirement for many listed companies.

Why do companies not report more internal incidents? Despite increased levels of corporate transparency, this corporate response may reflect the view that keeping the details of a fraud within the firm will help prevent collateral damage to the company's reputation, and limit the amount of management time and money being redirected to deal with the issue, with stakeholders, regulators and with other parties. However, when the perpetrator is outside the company and the news has a greater chance of becoming public, companies are more prepared to pursue the case with law enforcement agencies and regulators, in order to show good corporate governance and to reclaim as much of the loss as possible.

Yet despite the fears of negative publicity from involving law enforcement, the companies that did refer fraudsters for prosecution, whether internal or external, suffered no significant collateral damage and indeed, in many cases, saw a decrease in the collateral damage to their public relations, their business relations and their own working morale. Indeed, stakeholders and staff respond positively when they see a consistency of honest and fair action brought against those that have contravened the company's ethical guidelines (and brought their livelihood into disrepute).

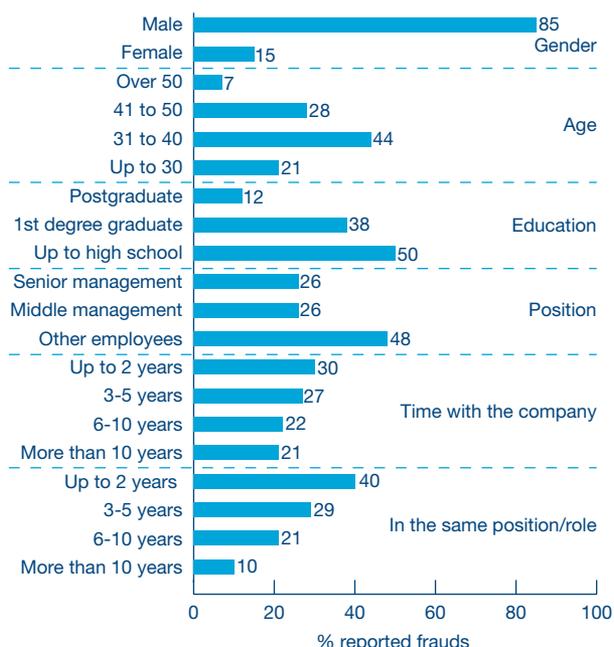
### The importance of consistency

Consistency in fraud risk management efforts is vital to achieving a positive impact. Our research shows that the actions brought against management are usually less severe than those brought against other grades (see figure 1.17).

In our view once an incidence of criminal wrongdoing has become known it is vitally important to signal to the staff that all perpetrators are treated the same way, regardless of their position within the company. There will nearly always be a certain level of negative impact on staff morale, but it is in just these cases that the company must show that actions against perpetrators from the senior management are the same as those brought against other grades within the business, and that there is not 'one rule for them and another for us'.

Our research shows that in the cases where fraud was committed by a senior manager, if referred for criminal prosecution, the chance of that fraud having a significant negative impact on staff morale dropped from 20% to 10%. Similarly, if the senior manager is sentenced, there is a significant impact on staff morale in only 7% of cases, but if the same perpetrator is seen to 'get away with it', the negative impact trebles to 21%. Finally, the degree of sentence handed to fraudsters

#### 1.16 Profiling the fraudster



despite fears of negative publicity, the companies that did refer fraudsters for prosecution suffered no significant collateral damage

from senior management is also a motivator, for when they are imprisoned or receive a heavy fine for their misdemeanour, the number of companies reporting a significant decline in staff morale drops by half. However, in cases where senior management has been handed a suspended sentence or put on probation, there is no change in the levels of negative impact on staff morale, implying again that management seems to be ‘getting away with it’.

### Recovery of lost assets

Over the years of measuring the recovery of lost assets, there has been little change, except a marginal increase in the numbers of companies recovering anything at all.

There are many reasons for this relative failure to recover lost assets. Companies are reluctant to embark on long recovery processes with uncertainty of success, especially where assets have been moved across borders.

However, there may be good reasons to pursue the assets regardless – firstly because it is not always possible to form a realistic view of the chances of recovery until the process gets under way, and secondly because a policy of always attempting recovery helps in the creation

of the right culture of deterrence if the assets are to be reclaimed from the perpetrator through civil actions.

Many companies choose to employ fidelity (or other types) of insurance against fraud. Because of the recent public and business interest in fraud and the crippling damage that it can be seen to cause to a company, premiums have grown. However, our research shows that insurance can have a positive impact, as those companies that claimed on it following a fraud were 33% more likely to recover more than 60% of their lost assets than those without insurance.

### Fraud in the future

Fraud remains an intractable problem. Levels have not dropped significantly 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, 11% of the companies consider it more likely that they will be victims of fraud over the next two years, which is three percentage points higher than the respondents believed in our 2005 research.

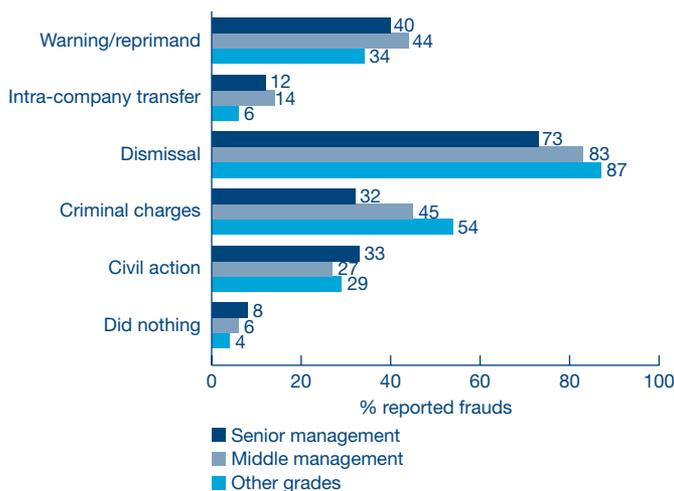
The results of this research have shown that the controls that have been implemented

will not be sufficient to mitigate the risk of economic crime on their own. Instead, our hopes rest in organisations establishing a culture that supports those controls with clear and ethical guidelines, engendering a loyalty to the organisation’s brand, and showing that every perpetrator, no matter what their position and function within the company, will be subject to equivalent sanctions.

This is particularly true for those organisations seeking to make dynamic expansions into the emerging markets to take advantage of preferential production costs and developing consumer societies. In many of these markets, corporate governance systems may not be as encompassing and exacting as in the developed markets and companies need to be aware of the risks that they face in the light of their regulatory requirements ‘back home’.

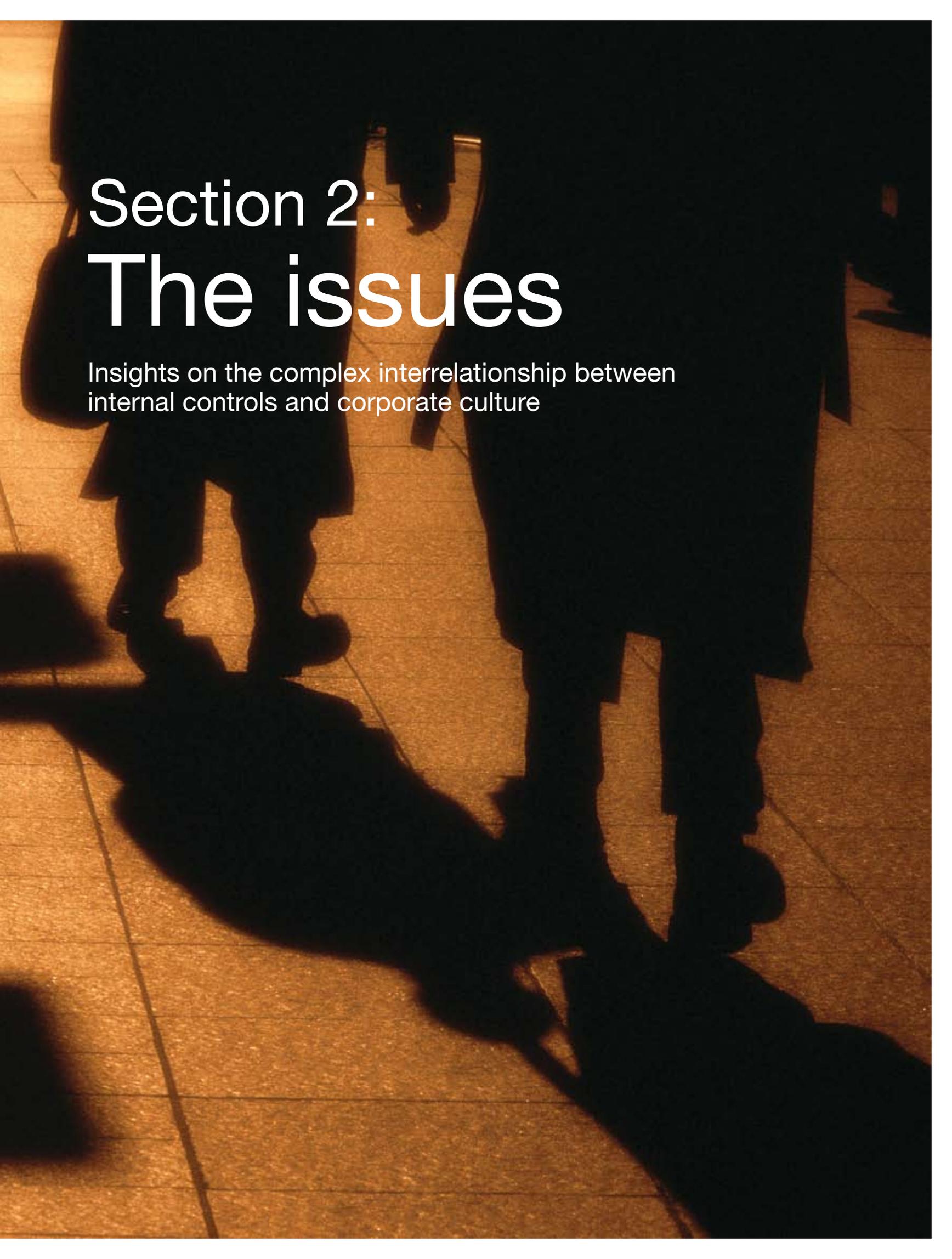
The fight against fraud is a constant struggle. Our biennial study continues to show that in order to assess and manage risk, a constant re-evaluation of all fraud risk management activities and the culture that supports them in every market of operation is vital to maintain a clear, competitive advantage and the confidence of all stakeholders. As with all crimes and unwanted business risks, consistent and effective prevention is better than after-the-fact reactions.

### 1.17 Companies bringing actions against internal fraudsters



the results of this research have shown that the controls that have been implemented will not be sufficient to mitigate the risk of economic crime on their own



The background of the slide is a photograph showing the lower legs and feet of several people walking on a light-colored, tiled floor. The lighting is low, creating long, dark silhouettes of the individuals. The text is overlaid on the upper portion of the image.

# Section 2: The issues

Insights on the complex interrelationship between  
internal controls and corporate culture

## Fraud's facilitators – individual propensities and corporate culture

Our survey results point to one incontrovertible fact: the crime of fraud remains intractable because of the many kinds of fraud and the correspondingly broad range of fraudsters who commit them. Fraud is also difficult to detect and stop because it contains a fundamental element of deceit.

Our research shows that in order for a fraud to occur, two preconditions must be present:

1. Perpetrators have deep-seated, personal reasons for engaging in criminal acts; they must have an incentive to commit fraud and be able to rationalise the fraud to themselves.
2. A company that is more likely to be victimised by fraud not only lacks sufficient controls to detect fraudulent activity but also lacks ethics, values, programmes and systems that discourage fraud, i.e., a well-developed culture, including systems that encourage and protect employees who expose fraud.

An analysis of the survey's overall figures indicates that holistic and regularly updated control programmes help limit opportunities for fraud. But it does not stop there. Controls combined with the company's ethical culture together play equally important roles in deterrence.

### Who are the fraudsters?

The survey shows that while fraud is committed by people at every level – and in practically every department – 'figureheads' within a business are responsible for 25% of all reported frauds and have been with the company for an average of seven-and-a-half years. Generally speaking, 85% of fraudsters are male, 44% are between the ages of 31 and 40, 50% have a school degree or less, and 38% possess at least a bachelor's

degree, while 12% usually hold a postgraduate degree, or higher.

Criminological research indicates that most fraudsters tend to be risk-takers, decisive, extroverted, career- or success-oriented individuals.<sup>1</sup> Paradoxically, it is precisely these traits that are also highly prized in management recruitment. Today's manager needs to possess a high degree of creativity and flexibility, qualities which can be successfully employed both appropriately and inappropriately.

### Individual propensities

If we look at the preceding conditions – personal reasons and corporate opportunities – our survey reveals a number of interesting results about individual motivations and self-rationalisations behind fraud (see box below).

#### Individual motivations:

- financial incentives/greed (57%)
- maintaining a lifestyle unsupported by their salary (36%)
- career disappointments (12%)
- prospect of being laid off or made redundant (8%)

#### Self-rationalisations:

- fraudsters' low temptation threshold (44%)
- apparent lack of awareness regarding the nature of their wrongdoing (40%)
- denial of the financial consequences of fraudulent act (26%)

most fraudsters tend to be risk-takers, or else very decisive, extroverted career- or success-oriented individuals... traits that are also highly prized in management recruitment

<sup>1</sup> For overviews Neal Shover, Andy Hochstetler, *Choosing White-Collar Crime*, 2006; David R. Simon, Frank E. Hagan, *White-Collar Deviance*, 1999; David O. Friedrichs, *Trusted Criminals*, 2nd. ed. 2004; Alan Doig, *Fraud*, 2006, p. 80ff.

Systems of procedures and controls do not necessarily counteract these motivations or self-rationalisations. However, well designed internal control systems supported by strong culture can work together to better mitigate the risks of individuals who may be motivated to inappropriately apply their talents. It is culture, in combination with procedure, which is effective against individual propensities toward fraud.

### The role of controls

Our survey results, combined with our experience, provide further insight into the role of controls in detecting and preventing fraud.

### The impact of fraud controls

Controls are an important element of the equation. The table below<sup>2</sup> shows that

when we compared companies that put more than five controls in place (i.e., Group B), their control networks were more effective in detecting fraud.

In contrast, companies in Group A (which had instituted an average of three modes of control) appear less aware of their vulnerability and consequently are not learning from whatever instances of economic crime it has been their misfortune to endure. Because such companies have weaker control systems in place, they predictably detect fewer cases of economic crime.

### The vicious circle of deceptive security – company performance on fraud prevention and detection

	Group A Companies with up to five controls	Group B Companies with more than five controls
Percentage of companies taking professional anti-fraud advice	12%	49%
Percentage of companies that reported detecting fraud	38%	47%
Average number of frauds detected	6	10
Average loss detected for all frauds per company	US\$ 901,285	US\$ 3,419,151
Average financial costs companies spent on managing frauds	US\$ 305,227	US\$ 701,832
Insurance taken to cover losses and costs from fraud	28%	47%
Percentage of companies with significant collateral damage and associated managing costs	26%	23%

In areas of common risks, such as asset misappropriation, our experience tells us that inattention and lack of discipline can be symptomatic of a cultural ambivalence towards correct behaviour that leads to an environment in which more devastating economic crimes – corrupt acts, participation in cartels, financial statement fraud – can occur. In effect, this is an indication of inadequate culture – and culture is the very thing which provides the best protection against a catastrophic economic crime event.

<sup>2</sup> More information about this can be found in Section 1 (see page 11).

### The Fraud Control Paradox

At first glance, it would seem reasonable that stronger controls would lead to an immediate drop in impropriety – but this is not necessarily true in the short run. It appears that what holds true in a larger criminological context applies equally well to companies seeking to detect fraud – the greater the sensitivity of a company towards economic crime, the more they seem to occur. In other words, if you do not look, you do not see; conversely, once you know what to look for and go looking for it, you are more likely to find it.

Over time, the effectiveness of a company's control system depends on

everyone knowing and understanding it. The gap between the number of detected and undetected cases closes because employees have a greater awareness of the controls in place, and potential perpetrators are more alert to the risk of detection. Controls are therefore most effective when everybody knows about them and, when a case of wrongdoing is discovered, the individual involved is dealt with in a manner appropriate to the offence, regardless of their position in the organisation.<sup>3</sup>

Nevertheless, while a company's control system will eventually lessen the gap between detected and undetected crime, unless it continues to evolve, eventually

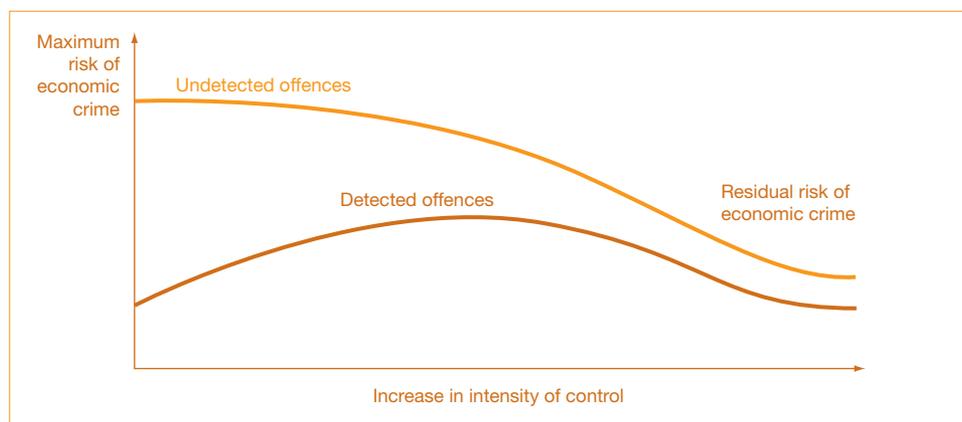
potential wrongdoers will find ways to circumvent it. When fraudsters and other wrongdoers know what to avoid, they are empowered to devise new and novel ways to pursue their criminal ends.

It is for this reason that whatever controls and detection systems or programmes a company puts in place must be constantly monitored and updated if they are to be effective.

### Key elements of effective controls

Implementing effective control systems requires a comprehensive understanding of the sources of fraud risk within the context of a company's domestic and global operations. Given that business growth and development is ever-changing, companies are challenged with regularly evaluating their operations, structure and systems to keep pace with change. While change and a willingness to take certain types of risk can lead to great opportunities, the same can increase a company's vulnerability to economic crime. To mitigate against this negative side of change, companies should regularly assess their vulnerability, evaluate their controls, and adopt programmes, systems and policies that meet their specific circumstances. An example of some key elements of effective controls against corruption and bribery is provided in the box which follows.

### The circle of deceptive security – company performance on fraud prevention and detection



if you do not look, you do not see;  
conversely, once you know what to look  
for and go looking for it, you are more  
likely to find it

**Key elements of effective anti-bribery compliance programmes**

1. Create a control environment with the right structure and tone:
  - CEO communication on the importance of compliance, and ‘zero tolerance’ for illegal acts and misconduct;
  - Establish a high-quality, compliance organisation that is well-staffed with clear processes and support systems;
  - Embed compliance into human resources processes including training, hiring, performance, promotion, ethics and compliance, and disciplinary actions.
2. Focus on the most important compliance risks:
  - Conduct risk assessments to identify high-risk areas including countries and/or business units, transactions, contracts and third party relationships;
  - Adapt processes based upon the nature and source of the risk.
3. Design compliance control activities to minimise risk of non-compliance:
  - Establish control procedures for high bribery risk areas;
  - Adopt protocols for investigating allegations of misconduct, illegal acts and non-compliance;
  - Develop independently tested monitoring programmes.
4. Establish processes and systems supporting compliance:
  - Ensure effective report on status, effectiveness and trends to key corporate governing bodies (i.e., Compliance Committee, Board of Management, Audit Committee and Supervisory Board)
  - Embed compliance into the IT systems.

**The impact of ethical guidelines and compliance programmes**

Our survey results clearly show that companies’ that make use of effective ethical guidelines and compliance programmes are much less vulnerable to economic crime. As the chart below shows, companies with these programmes are less likely to be victimised. The impact of such programmes on a company’s vulnerability to crime is significant, whether it is asset misappropriation, accounting fraud, corruption or money laundering (see figure 2.1).

**Breeding grounds for discontent**

Clearly, the development and deployment of internal controls and risk management systems is vital if the risk of fraud is to be reduced, but they can only go so far. There are many forces, both good and bad, at work in the formation and ongoing ‘life’ of a company’s culture; but there are some quite specific, easily-identifiable factors that erode the positive influence of culture and create the kind of environment that contributes to wrongdoing.

**The role of corporate culture**

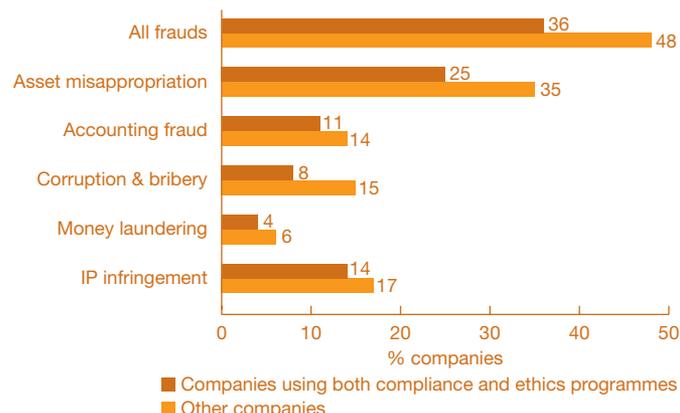
What is ‘corporate culture’? For Charles Hill and Gareth Jones it is ‘the specific collection of values and norms that are shared by people and groups in an organisation and that control the way

they interact with each other and with stakeholders outside the organisation’.<sup>4</sup>

This section of the survey will examine some of the critical components that make up a company’s culture and their respective roles in preventing (or discouraging) corporate crime.

companies that make use of ethical guidelines and compliance programmes are much less vulnerable to economic crime

**2.1 Companies with both ethical guidelines and compliance programmes report suffering fewer economic crimes**



4 Charles W. L. Hill and Gareth R. Jones, (2001) Strategic Management 5th Edn, Houghton Mifflin, MeansBusiness, Inc.

One factor in the creation of disaffection amongst employees is the pressure to perform or produce and our survey showed that this was an incentive in 13% of cases, increasing to 22% in the case of senior management's involvement. Obviously, high productivity and exemplary performance are always desirable, but when management expectations are unrealistic it is easy for employees to justify an 'anything goes' approach to achieve company goals.

What can be particularly damaging are situations where employees are unsure about what to do when they become suspicious about the conduct of fellow employees or are themselves confronted with ethical dilemmas. If a company does not provide clearly-defined channels of communication for its employees it may run the risk of sending the wrong message: that management does not want to hear about problems and/or ethical employees may either be ignored or find themselves the victims of management retaliation.

Any one of these factors may be enough to engender the kind of resentful, 'get-even' mentality that seizes many fraudsters; but, taken together they represent a distillation of negative forces that makes for a positively toxic corporate culture – one in

which 'anything goes', 'who cares', 'and who is going to catch me anyway', let alone 'call the authorities' attitudes prevail.

### Setting the tone at the top

The role of upper management in creating and transmitting both an ethical code of conduct and responsible behaviour are crucial. As Sam Di Piazza, PricewaterhouseCoopers' CEO, pointed out, 'People in an organisation pick up quickly on how the CEO and other senior executives deal with individuals and situations that may not conform to the ethical code. The board also has something at stake: it is the responsibility of the total leadership, including the board, to infuse an organisational culture of ethics, and this challenge includes communicating effectively.' Our study supports this: in 30% of cases involving a member of senior management, there was significant damage to ongoing staff morale in the company.<sup>6</sup>

A company's code of ethics should be clearly articulated and conveyed to each and every employee. Everyone, regardless of their rank or position – from the CEO and the Board of Directors down to the

mailroom personnel – should be aware of how their company's code of conduct works: what it allows, and what it does not.

### Senior management accountability

While some companies refer fraudsters from within senior management for criminal prosecution, many do not.

Our survey finds that there is a significant difference in the way companies deal with senior managers involved in fraud and the way in which they approach other employees. We find, for example, that criminal charges are brought against senior management less frequently when compared with employees lower down the corporate ladder. More telling, perhaps, is the finding that, compared with the numbers in our 2005 survey, companies are now limiting their response to warnings or reprimands when the offenders come from senior management.

Yet when senior management is not punished appropriately – and some may even say gravely – the impact on staff morale can be significant. As discussed in Section 1, in cases where fraud was committed by a senior manager, if referred

obviously high productivity and exemplary performance are always desirable, but when management expectations are unrealistic it is easy for employees to justify an 'anything goes' approach to achieve company goals

for criminal prosecution, the chance of that fraud having a significant negative impact on staff morale dropped from 20% to 10%. The perception that management 'gets off lightly' fuels employee discontent and erodes corporate culture.

### The impact of whistle-blowing systems

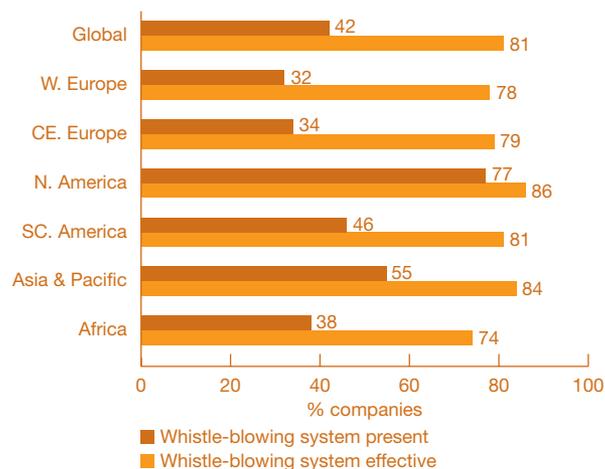
As the chart below shows, in virtually every region of the world whistle-blowing is playing a role in uncovering the activities of wrongdoers. More and more companies are now promoting whistle-blowing policies as an integral part of their risk management programmes (see figure 2.2).

We believe whistle-blowing systems that are both well designed and properly implemented can play a decisive role in uncovering criminal activity. This is reflected in our respondents' very positive views on their own whistle-blowing system's effectiveness. When this detection tool is correctly implemented, it has the strong potential of effectively uncovering more fraud – increasingly replacing the chance element of anonymous tip-offs that, in our study, were responsible for detecting fraud in 34% of reported cases.

#### 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 certain employees can report incidents outside their chain of command – avoiding their supervisor, department head, 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 both a toll-free call 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 personnel issues and Security or Risk Management for more serious issues such as suspected fraud.
- Include controls for targeting certain situations that may require immediate steps to prevent further risk or damage.
- Provide clear governance expectations about how matters will be reported to the ultimate 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 not only for reporting misconduct, but also for asking questions and receiving guidance.
- Track trends that 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 doesn't abide by its own rules, from the top down, will never work effectively.
- Train and periodically update all company employees about the whistle-blowing programme, disciplinary policy and the company code of conduct.

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



in virtually every region of the world, whistle-blowing is playing a role in uncovering the activities of wrongdoers

There is no substitute for the perceptiveness and acuity of the individual when it comes to discerning those patterns of odd behaviour, unlikely coincidences and atypical work methods that often signal the presence of economic crime. We must add, however, that it is important for companies to promote whistle-blowing procedures as a pro-active means of protecting the brand (and thus the company as a whole), and not as a way for employees to settle old scores or turn in colleagues or managers.

### Reporting fraud to the authorities

Our research reveals that reporting an offence to the prosecuting or regulatory authorities had fewer negative effects than once anticipated. While many companies in the past clearly chose not to involve law enforcement agencies once a fraud had been uncovered, our research reveals that

those companies that did call in the authorities suffered less reputation and quantifiable damage. The apparent past perception of the danger of ‘collateral damage’ or fallout is fading.

Apart from the negative effects of litigation issues, many companies report that when they have pressed criminal charges against fraudsters they have not only suffered less public relations damage and less impairment to their outside business relations, but employee morale could actually have been improved.

These developments may be due, in part, to the recent focus on corporate governance, and the requirement for companies to show regulators and stakeholders that, in such matters, they are ethical, responsible corporate officers who put a premium on honesty.

### Conclusion

One clear fact is apparent when we look at the results of our 2007 survey: corporate culture is a vital element in whatever fraud risk management programmes a company adapts. Keeping this in mind, we recommend that companies consider the following points as they move forward in developing fraud control programmes and strategies:

- Replace one-off risk mitigation programmes (i.e., one-off review of agent relationships) with comprehensive compliance programmes that are fully integrated into all components of business operations.
- Pro-actively monitor vulnerabilities to fraud. It is not so much a question of always expecting the worst, but being prepared for the unexpected; and, should it occur, being ready with an effective fraud response plan.

**the best-laid plans and procedures are unworkable if they are not championed by management and watched closely by every employee in the company – without exception**

- Developing a strong ethical culture that is clearly evident to all employees. This can be accomplished through setting the right ‘tone at the top’, encouraging company loyalty, providing processes whereby employees can report concerns (i.e., whistle-blowing systems), and by clearly showing that the penalties fraudsters incur – no matter what their position in the company hierarchy – are serious.
- Be sensitive to the issues that individual employees might be faced with, such as the wrongdoing of a colleague.
- It is impossible to eradicate economic crime; like the Hydra of myth, cutting off one head merely allows another to grow. This does not mean, however, that prevention is impossible and should therefore be abandoned. On the contrary, companies large and small should take all the precautionary steps they can to deter fraudsters – and those who merely contemplate the crime.
- A comprehensive understanding of fraud risks sources and controls provides a foundation for making informed decisions about how and where the other risks – the right risks for building business – can be taken.

Risk exists. Each organisation must define which risks must be mitigated or taken to protect the business without sacrificing reward – an explicit risk appetite. Fraud is just one of many risks an organisation must consider as part of this risk appetite. But, as the GECS suggests, fraud prevention is not merely a question of the right control functions but rather part of the holistic approach to risk – controls, culture, ethics and performance. If an organisation’s **risk appetite** is clearly articulated in the **strategy**, driven into the **culture** from the top down and consistently applied to decision-making, **risk-taking** can drive performance, yield value and properly address threats such as fraud.

risk exists – each organisation must define which risks must be mitigated or taken to protect the business without sacrificing reward





# Section 3: The emerging markets

The perceptions and experience of experts who are confronting the risk of fraud in some of the fastest growing economies in the world

We are often asked about economic crime risks in the developing markets and in particular in those countries that offer the most outstanding opportunities, i.e., Brazil, China, India, Indonesia, Mexico, Russia and Turkey (a group which PwC terms the 'E7', or 'Emerging Seven').<sup>1</sup> Here we combine the experiences of more than 1,500 E7 experts who contributed to our research programme (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.

### New ventures – new opportunities for fraud

For many companies, the opportunities offered by the E7 economies are so great that there is often a need to move quickly to take advantage of the potential cost benefits or market opportunities that are available. However, it is during these times of dynamic change that businesses are

particularly vulnerable to fraud. Our research reveals that companies that experienced changes in structure, which are typical during periods of overseas expansion, were more susceptible to fraud than those that operated in a stable environment (see figure 3.1).

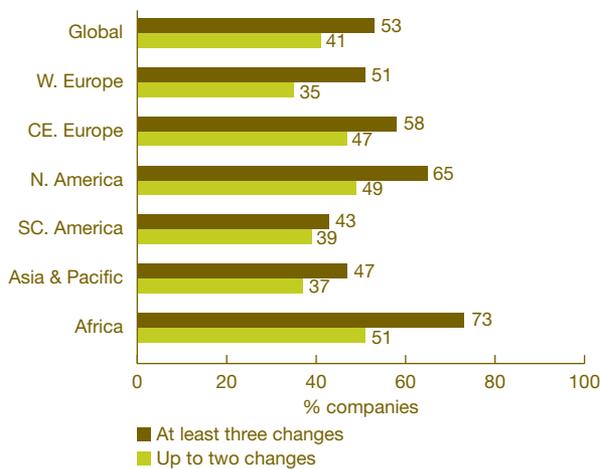
In all of these cases, there were changes in operational processes, procedures and systems; personnel changed; roles, positions and responsibilities were reorganised into new configurations; and, of course, there were new and changing customers and suppliers. In situations where managers and staff lack familiarity with systems, roles, customers and suppliers, the kind of irregularities that may otherwise have caused a raised eyebrow in a more familiar or better established 'home' environment may well go unnoticed. Worse, the situation may present an opportunity for fraudsters to take active advantage of the company.

For example, take the issue of companies operating different accounting systems.

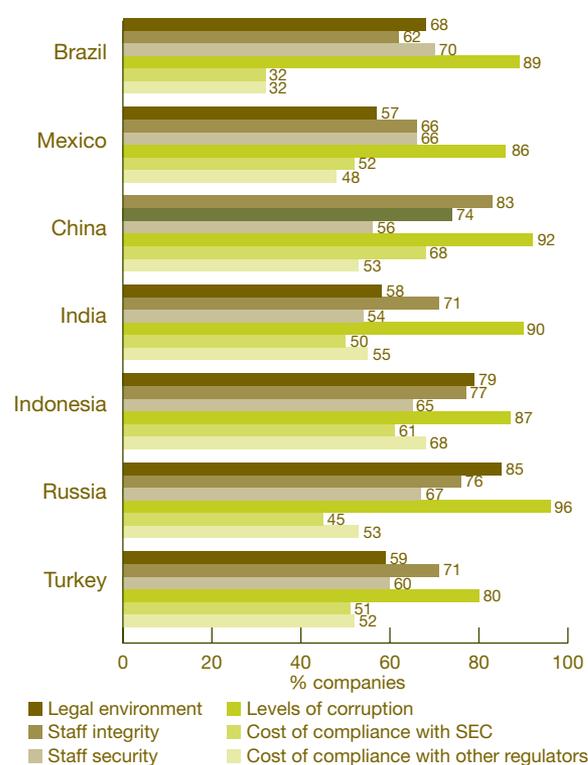
Our research reveals that companies in which parent and subsidiaries employed different accounting systems were more susceptible to fraud (61% of cases) than those operating a unilateral system (52% of cases). This is not surprising, for while a quality accounting system can act as a very effective first line of defence against many common fraud schemes, the gaps that often exist between systems certainly increase the opportunities for fraud to flourish.

Or take the issue of suppliers. Companies moving into an E7 region, or acquiring a local company, must rigorously vet not only new suppliers, but also existing ones. Conflicts of interest often arise in the E7 countries, where buying or selling from friends or family to pass economic benefit outside the company is commonly viewed as a basic business practice. It is the way that business is done, and sometimes has been for centuries. Plus, it is important to remember that a number of the E7 markets have not been open to free trade for very long.

### 3.1 Companies reporting fraud that have undergone significant structural changes



### 3.2 Experts' concerns about fraud issues in the E7 markets



<sup>1</sup> PwC's head of macroeconomics, John Hawksworth, estimates that by 2050 the E7 economies are likely to be 25% larger than the G7's at market exchange rates, and 75% larger in terms of purchasing power parity. ('The World in 2050. How big will the major emerging market economies get and how can the OECD compete?')

### The perceptions and the realities of fraud in the E7

So with a move into the emerging markets likely to expose your organisation to increased possibilities of economic crime, what are the types of fraud that you are likely to experience and how does the threat differ from the rest of the world?

The experts in E7 investment interviewed for our survey perceive significant risks associated with levels of corruption, staff integrity and legal environment in the emerging markets for which they have direct responsibility (see figure 3.2). These types of economic crimes are no different from those that are to be found in the developed economies. The difference lies in the extent to which – because of the legal, political, social, economic and cultural environment in which these companies operate – they permeate private business; and, of course, the effectiveness of the internal controls and corporate cultures that these businesses possess to mitigate such risks.

The concerns faced by experts investing in E7 markets are borne out by ‘in country’ companies’ assessment of the most prevalent fraud type. Both groups – the E7 companies surveyed and the experts investing in the E7 countries – perceive corruption to be the most significant economic crime threat (see figure 3.3). Further, in all E7 countries, the experts consider staff integrity to be the second or third most widely held concern. Examining the actual levels of reported fraud in the E7 countries, we see consistently high reported incidents of asset misappropriation – a solid indication that concerns about staff integrity by E7 experts are well founded (see figure 3.4).

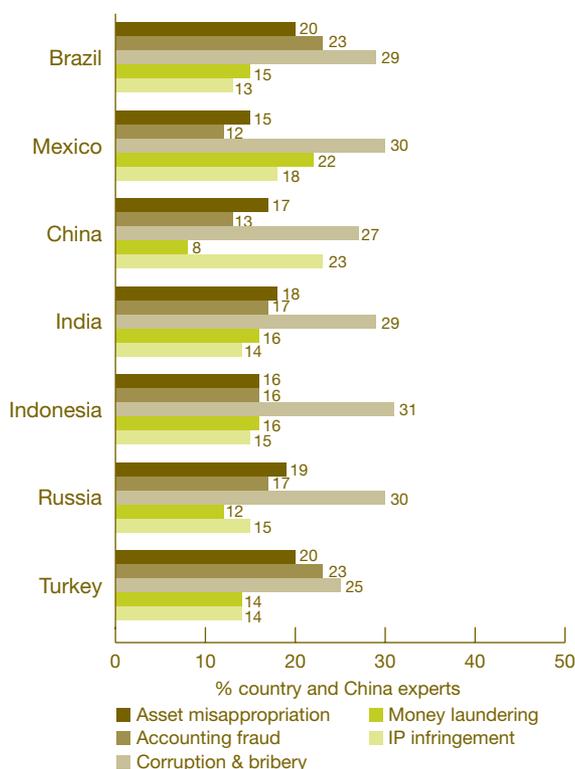
It is interesting to note that regulatory compliance of any type is perceived as the lesser risk. However, while this no doubt reflects the experience of respondents over the past two years, we anticipate that the regulatory activity will increase in many jurisdictions, putting increased pressure on compliance systems in the near future. Already, companies which settle allegations of economic crime in the United States are

discovering follow-on actions by authorities in other nations with a nexus to the issue.

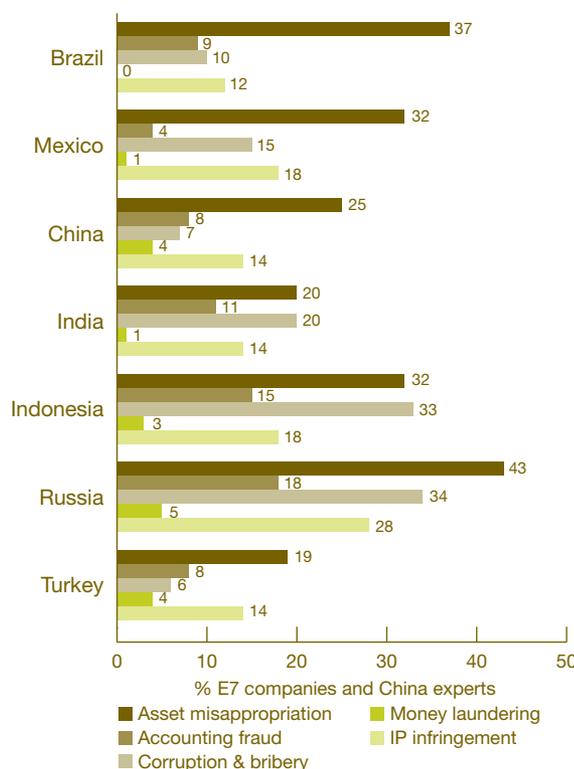
The perceived levels of fraud versus actual reported incidents in the E7 countries reflect a strong consistency with global results – except that corruption and bribery and, to a lesser extent, money laundering, is perceived to be greater. With regard to actual reported incidents of fraud, E7 levels approximate the global statistics, again with the exception that corruption and bribery and asset misappropriation are reported more frequently in the E7 than the rest of the world. It is interesting to note that our own experience and the results of Transparency International’s 2006 Corruption Perception Index suggest that the perception levels provided by our E7 experts reflect a level of corruption threat that is surprisingly consistent.

While the perceived levels and reported number of incidents are quite similar to the global findings in most areas, this does not fully explain the level of concern exhibited by our expert respondents about the risks in E7 countries. The answer may

3.3 E7 companies’ and China experts’ perceptions of the types of fraud most prevalent in the E7 markets



3.4 Types of frauds actually reported by E7 companies and China experts



lie in the financial losses reported by our experts – which tell a different and more worrying story. The total losses reported by the companies that took part in our survey amounted to more than US\$ 4.2 billion over the course of the previous two years. Over 45% of that figure was lost by companies operating in the E7.

**Total losses reported by all respondent companies: US\$ 4.2 billion**  
**Total losses reported by E7 companies: US\$ 1.9 billion**

In the first section of this report we also explored our respondent companies' average losses from fraud, and this amounted to US\$ 2,420,700. In comparison, the average losses reported by companies operating in the E7 amounted to more than double this.

**Average losses over two years reported by all respondent companies: US\$ 2,420,700**  
**Average losses over two years reported by E7 companies: US\$ 5,053,286**

Average loss (US\$)	All respondents <sup>2</sup>	E7 respondents (including China)
Asset misappropriation	859,646	2,915,419
Accounting fraud	954,798	3,406,917
Corruption and bribery	297,071	1,977,762
Money laundering	230,544	374,326
IP infringement	1,766,215	2,180,180

Indeed the average losses for each type of crime also make sobering reading.

But, of course, the drain on a company's finances does not just rest with the losses. One must also consider the potential collateral damage to staff morale, supplier relations and the brand, as well as the financial and time cost of managing the fallout from such matters. Again, in the E7, these costs have been shown to be one-and-a-half times those in the rest of the world.<sup>3</sup>

**Average cost of managing frauds over two years by all respondent companies: US\$ 550,356**  
**Average cost of managing frauds over two years by all E7 companies: US\$ 825,982**

### An illusion of safety?

Yet despite this considerable threat to the financial and operational security of business, almost half (45%) of our experts did not factor economic crime as a risk criterion for assessment prior to their investing in E7 countries. Why? Perhaps because many of those companies regard fraud as such an endemic problem in these markets that it is regarded as just one of the 'obstacles' that has to be overcome in order to do business. Plus, from a risk vs return point of view many companies seem to take the position that the damage is more than off-set by the investment opportunities being offered.

On the other hand, it is encouraging to see that, for 55% of respondents, fraud

some companies from the developed economies have found to their consternation that trying to impose Western controls simply does not work

<sup>2</sup> Global total average loss excluding E7.

<sup>3</sup> The issues of financial losses and collateral damage are dealt with on page 9 of this study.

is regarded as an important consideration in the investment risk review process.

For example, staff security was rated of paramount importance in both Russia (67%) and Brazil (70%). An apparent lack of faith in an independent and legal environment also provides concerns for those investing in China (83%) and Russia (85%), which may, to some extent, be shaded by preconceived Western notions regarding the effectiveness and independence of institutions (see figure 3.2).

### Be prepared

Yet, as the saying goes, there is no smoke without fire, and this is never more relevant than when reviewing the risks that staff or a business may face when entering a new market. So for businesses looking to invest in the emerging markets, we recommend the following:

1. Be sure that you understand the particular fraud risks that you will face in your chosen market, particularly if you are a listed company and subject to regulations like the Foreign Corrupt

Practices Act ('FCPA') or similar legislation. Consider seeking advice from a local, professional forensic consultant who can inform you of the realities of the situation.

2. Prepare fraud risk management programmes that specifically address those fraud issues in particular, rather than expecting your own country's tried and tested models to be effective in every constituency and every eventuality.
3. Conduct rigorous due diligence on any acquisitions, or prior to any partnerships or joint ventures. The cost of doing this in advance is a great saving on the costs of withdrawing once the programme has been established for some time.
4. Be prepared for the actions you need to take should a business partner, an acquisition, a joint venture partner or a member be shown to be behaving inappropriately.

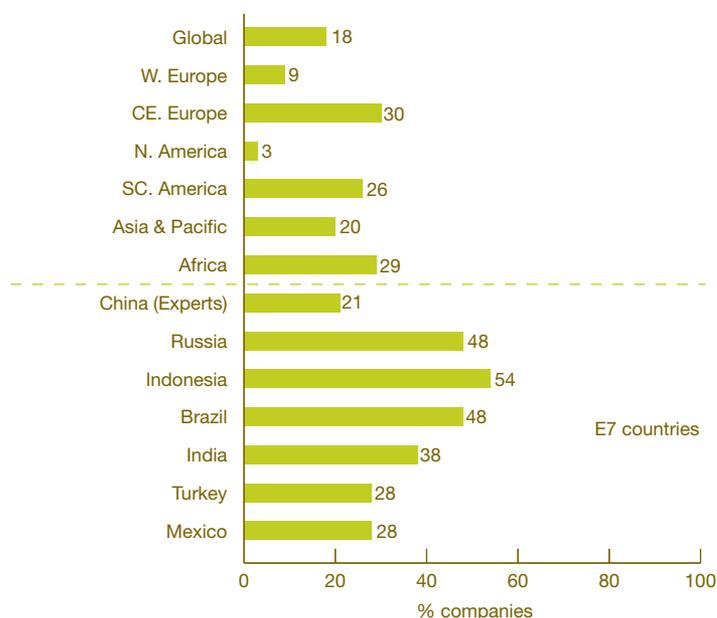
Finally, recognise that some companies from the developed economies have found to their consternation that trying to impose Western controls simply does not work.

This 'one-size-fits-all' mentality is mostly found in those companies that think that they can sort out all the problems once they 'hit the ground' in the E7 market.

### Corruption – a genuine threat?

'Honesty stands at the gate and knocks,' said the 16th-century English author Barnabe Rich 'and bribery enters in.' Certainly, the E7 experts who took part in our survey perceive corruption and bribery to be the most prevalent economic crime threat in the emerging markets, but is this just a spectre, an illusion that business in certain countries can only be done when money (or its equivalent) changes hands, or is bribery really the unavoidable cost of doing business in many parts of the developing world? Outside Western Europe and North America, 20% to 30% of respondents reported encountering circumstances where they were asked to pay a bribe (see figure 3.5). In comparison, 21% to 54% of companies from the E7 countries reported encountering circumstances where they were asked to pay a bribe.

3.5 Percentage of companies asked to pay a bribe



Further, across the E7 markets, over one third of companies (34%) believed that they had found themselves in a position where they had lost a business opportunity to a competitor which they think may have paid a bribe, compared with a global average of 24%. This is significantly higher than the developed markets of North America (6% of companies) and Western Europe (14%) which have well-established anti-corruption conventions that are supported by a culture that rejects corruption (see figure 3.6).

Our findings reveal further interesting results: if we compare the number of companies in the E7 which felt that they were asked to pay a bribe at least once (over a two-year period) with those that had no such requests, the differences are clearly significant. Companies that are asked to pay a bribe are likely (45% Brazil/47% Mexico) to very likely (70% Russia/ 71% China) to lose the opportunity. This suggests that a request to pay a bribe is a significant indicator of a market that is not operating according

to competitive norms. It appears to indicate situations in which business relationships will likely not be established on the basis of product or service quality and price, but instead on corrupt criteria. The inverse finding – that companies not asked to pay bribes lose fewer opportunities to a competitor – confirms this finding. Thus, it appears that in the E7 context, finding that one’s company is being asked to make bribe-like payments is significant evidence that the business may well be let on a non-competitive basis and an unsuccessful outcome is likely (see figure 3.7).

In certain instances, the percentage of companies not being asked to pay a bribe may be a result of something as simple as the fact that a company has a good reputation, i.e., its standing as an ethical and honestly-run concern meant that it was never asked to pay a bribe and therefore suffered little in the way of lost opportunities. By the same token, the companies which felt they were asked to pay may not have been as well known in

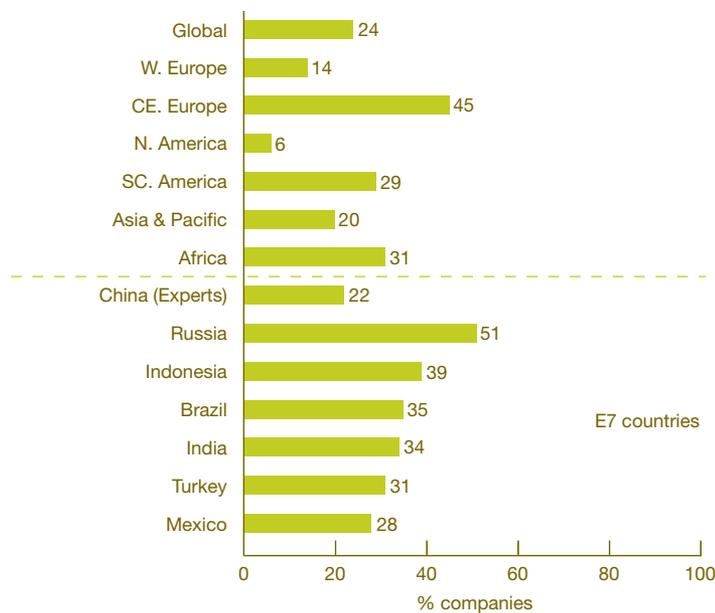
the marketplace (and therefore worth the risk, from the point of view of those bribing), or may simply have misinterpreted unfamiliar cultural norms and projected an ambiguous or ill-defined ethical appearance.

Yet, if companies feel that they have lost out by not acting corruptly (as figure 3.6 shows), should they consider turning a blind eye to instances of corruption in order to secure contracts?

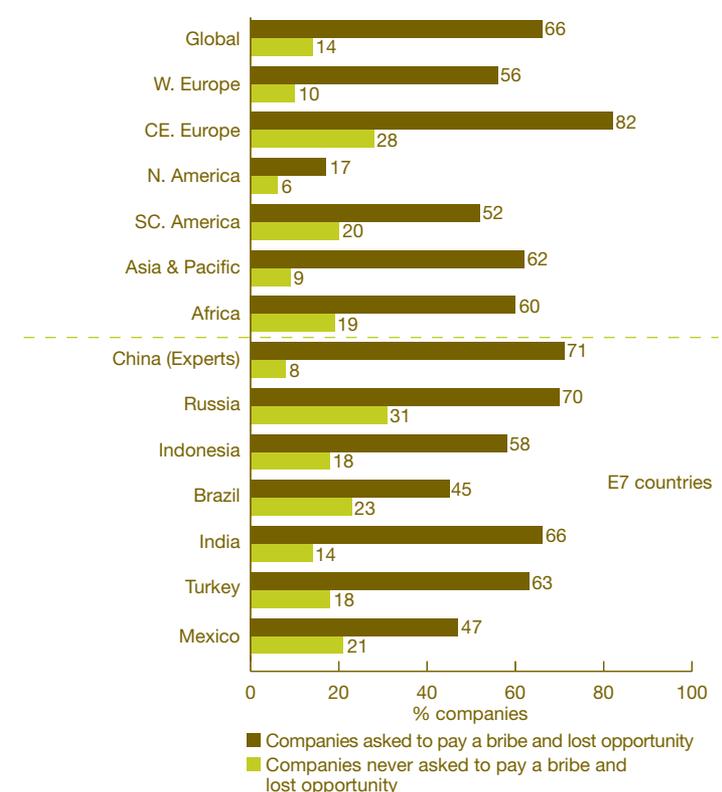
The answer is simply, no. And for four good reasons:

Firstly, for companies listed in the developed markets, the threat of regulatory action and the subsequent costs of remediation and any sanctions can be crippling. For example, the US Foreign Corrupt Practices Act, which requires domestic and foreign companies listed in the US to accurately record their transactions, imposes harsh penalties on companies that contravene its statutes. It is therefore vital for companies to create and

**3.6 Companies that lost an opportunity to a competitor who may have paid a bribe**



**3.7 Companies asked to pay a bribe that lost an opportunity to a competitor**



deploy effective anti-corruption measures in order to reassure the SEC (or other regulators) that they are doing all in their power to conform to the requirements, and spirit, of the laws (even if they should fall foul of corruption).

Secondly, the ethical standing and good character of an organisation can actually be part of a defence strategy (or protective mechanism) that can effectively shield a company against the offers of corrupt outsiders. Once again, this underlines the importance of a company possessing a visible and unassailable culture of honesty and fair dealing. But that 'ethical culture' must, somehow, extend to and embrace a company's local workforce too. Regardless of how ingrained or 'normal' the practice of bribery may be in a particular culture, it is important that the indigenous talent is shown how truly destructive the practice really is – to the company in which they work, to their community, and even to the economic well-being of their country and the generations that will come after them.

Thirdly, our research reveals that effective and well-implemented anti-corruption programmes are very efficient at cutting corruption levels and deterring fraudsters. For example, the companies in the E7 which had implemented effective anti-corruption controls in conjunction with strong, clearly understood ethical guidelines said they suffered up to 50% fewer incidents of corruption than other companies (see figure 3.8).

Fourthly, and uniquely, our research shows that incorporating an anti-corruption programme into your business activities does not have a detrimental effect on business development activities. Indeed, far from losing opportunities by not paying a bribe, our research shows that only 18% of the companies which had implemented anti-corruption programmes and ethical guidelines lost opportunities they had pitched, compared with 25% of the companies which had implemented none.

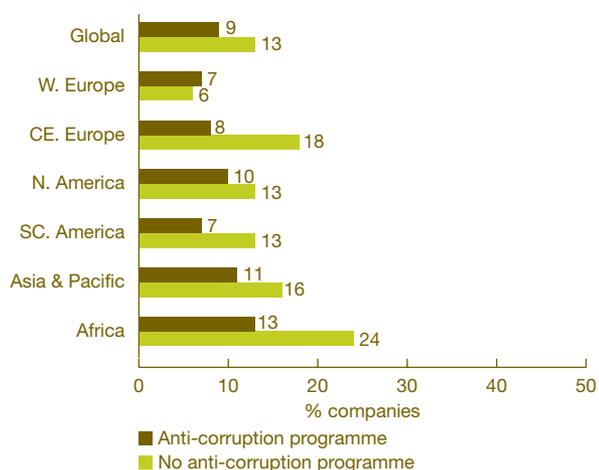
All of which goes to show that compliance will not kill your business. On the contrary: far from limiting the resourcefulness of employees, these compliance programmes encourage them to become more competitive and resourceful by focusing on the benefits of the service, product or contract on offer.

### China – the dragon spreads its wings

China has been of particular interest to our clients in recent years. We decided therefore to conduct in-depth interviews with senior executives who had first-hand experience of fraud issues in China and we sought their opinions and knowledge in order to compile this section. Our interviews cover more than 500 global companies familiar with operating in China.

Before we examine the different risks that need to be addressed when doing business

### 3.8 Companies with anti-corruption programmes suffering corruption



incorporating an anti-corruption programme into your business activities does not have a detrimental effect on business development activities

in China, it is worth noting that the country is, indeed, truly vast – it is the third largest country in the world, next to Russia and Canada – and despite the odd wobble or two has maintained an annual economic growth rate of around 8-9% per year over the last decade. (By way of comparison, the 2005 annual growth rate in the UK was 1.8%, in the US 3.5%, in Belgium 1.5%, in Germany 0.9%, in Italy 0.1%, and in Canada 2.9%.) In fact, China’s economy is now the world’s fourth largest, and its economic output for 2006 was US\$ 2.68 trillion. In addition, and true to the government’s stated goal of reforming its business policies, around 65% of China’s GDP in 2006 was generated by the private sector, a fact clearly apparent in a country awash with new construction projects, new companies (both foreign and domestic), and new business initiatives. In January 2007, Bloomberg reported that the Chinese stock market had hit the US\$ 1 trillion mark for the first time in its history, and by August 2007 this figure had grown to

approximately US\$ 2.5 trillion, according to government statistics.

With a population of some 1.3 billion people – and rapidly developing industries such as iron and steel, coal, textiles and apparel, petroleum, cement, chemical, toys, food processing, automobiles, consumer electronics and information technology – it’s easy to see why China is so attractive to outside investors and foreign companies.

Our survey results clearly show that the two greatest fraud risks to be faced when operating in China are perceived to be corruption and those frauds that fall under the category of IP infringement, although the former is not greatly different from the perceived threat in the other emerging markets (see figure 3.9).

When we asked our survey respondents whether there had been a foreign perpetrator involved in the crimes they had experienced in their own country’s

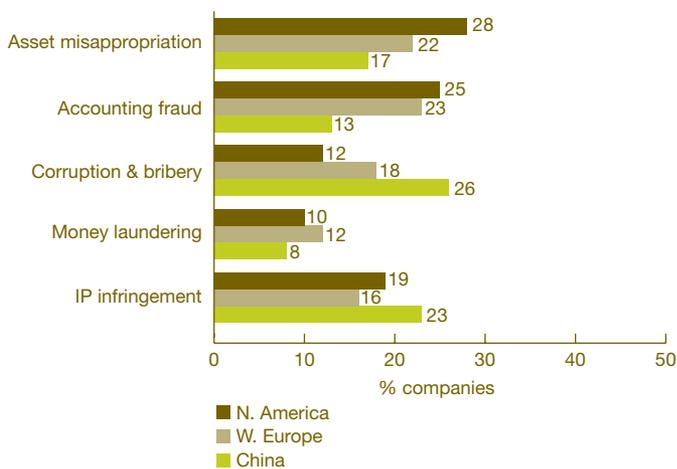
operations, the fraud risks related to doing business with China become even clearer:

- Of the 21% of corruption cases that involved a perpetrator located overseas, 17% of those involved a perpetrator from China.
- Of the 41% of IP infringement cases that involved a perpetrator located overseas, 44% of those involved a perpetrator from China.

### Managing the risks of doing business with China

There is an evident need to prepare for the fraud risks associated with doing business with or in China at this time. And while it is encouraging that 15% of those that are doing business there are considering what control measures to put in place in comparison to an average of 8% of companies elsewhere in the world, only just over a quarter of companies

### 3.9 Companies’ concerns over fraud risks – comparing China and the developed market regions



65% of China’s GDP in 2006 was generated by the private sector, a fact clearly apparent in a country awash with new construction projects, new companies (both foreign and domestic) and new business initiatives

(27%) had strengthened their existing controls, and less than a fifth (17%) had put in place any new controls that were suited to the specific risks of the region.

This may be because operations in this emerging market are so new, but with perceived levels of corruption higher than the global average, Western-listed companies must consider dealing with this issue at the earliest opportunity.

One of the major problems for foreign companies doing business in China is the perceived lack of effective legal protections, which extend to mergers and acquisitions, retaining land-usage rights, and – especially problematic, even now – protecting both private property and intellectual property. Foreign companies have to recognise that one fundamental difference between doing business in China and, say, the EU or the US, lies in the legal and regulatory systems. Western-based investors often find it more difficult

to interpret Chinese laws with the same degree of precision they would in the EU or US.

However, Beijing is now making great efforts to reduce the amount of red tape businesses have to endure.

### Cultural issues

In all of our considerations we must take into account the importance – and the effect – of the relationship-based way of doing business that is common in the Asian, African and Latin American economies. To do business in China, for example, a company's representatives must have 'guanxi', that is, good, strong, one-to-one personal relationships. With the right relationships in place a company can achieve a high success rate, but without those relationships, a company may expend a great deal of effort without achieving success.

One very important cultural element is 'face'. Targets or stretch budgets set from abroad may be seen locally as a 'must achieve', and consequently there may be a far greater imperative to meet these targets one way or another. The magnitude of this need to 'hit the numbers', and what can happen when there is a shortfall, cannot be overstated. It is an easy step sideways into fraudulent behaviour for managers who feel that they will rise or fall depending on the results they produce.

One should also take into consideration the fact that financial systems in the E7 countries tend to be far less sophisticated (and thus less exacting) than in the developed markets. Many companies still operate manual entry accounting systems and for foreign invested entities there will generally be at least two sets of books – (one for local reporting under PRC GAAP, one for the overseas investor under its own GAAP or IFRS), and for domestic entities the possibility of a third set of records

to do business in China, for example, a company's representatives must have 'guanxi', that is, good, strong, one-to-one personal relationships

showing higher profits than reported to the tax authorities – which, needless to say, creates the opportunity for ‘error’.

Accounting fraud, for instance, is not always regarded as such in China, but as an ‘error’ and is therefore not always reported. At the same time, the language barrier and different GAAP can also make it difficult for non-Chinese-speaking foreign auditors to spot these ‘errors’, or alternatively for local management to understand the international accounting requirements.

We must also include, as part of this discussion, the subject of governance, which, in many E7 countries, tends to be relationship-based: i.e., the subordinate does as they are told by their manager often without question. In these cases, there is little understanding of ‘principles-based governance practice’ and Western companies that have invested or are intending to invest in these markets may need to do a lot in the way of training and

education in order for local management and staff to understand how they are expected to operate.

### Computing the losses

The most pressing problem for many non-Chinese companies is, as we mentioned earlier, IP theft. Companies in the US, the EU, Japan, Singapore and elsewhere have seen their products – which are supposedly protected via trademarks, patents and copyright – illegally copied in China. According to our survey some 23.5% of foreign companies in China said they had been the victims of IP infringement; and 44% of IP infringement cases (worldwide) that involved a perpetrator overseas involved a perpetrator from China. It has been said that the global distribution of pirated products generates as much as US\$ 500 billion a year, 70% of which originates in China, although such figures are obviously speculative. However,

according to the China ‘experts’ surveyed, their own companies in China lost a total of US\$ 191,118,688 to fraud over the last two years. On average each company lost US\$ 1,790,685. (This is a little less than the global average of US\$ 2,420,700, but this may be because Chinese companies do not always have the kind of controls, processes and culture in place to be able to accurately assess what has been lost.)

So, how does the Chinese government regard these matters? China’s assistant Minister of Public Security, Zheng Shaodong, speaking at a recent symposium said that ‘China has seen an increasing number of cross-border economic crimes in recent years, especially in fields such as intellectual property infringement and money laundering.’

Mr Zheng also said that over the past seven years Chinese law enforcement

44% of IP infringement cases (worldwide)  
that involved a perpetrator overseas  
involved a perpetrator from China

agencies had uncovered some 400,000 instances of economic crime and had arrested 370,000 suspects, recovering approximately 100 billion yuan (US\$ 13.2 billion) in the process. There is obviously a willingness on the part of Beijing to admit that a problem exists and that it has to be tackled. As Minister Zheng pointed out: 'Many economic crimes are either not detected or unable to be investigated, and this represents a threat to social harmony.'

China is not alone among developing countries in having to contend with such problems. However, its remarkable success in the last few years has made it possible for economic crime to take root, especially bribery. In fact, according to China experts surveyed, 17% of their companies in China suffered from instances of corruption and bribery. By way of comparison, 14% of these companies experienced some form of asset misappropriation, and only 6% of them had uncovered any instances of accounting fraud.

### And the future?

So, what of China's future in the ongoing fight against economic crime? To quote China's own sixth-century BC philosopher Lao Tzu, 'Those who have knowledge, don't predict. Those who predict, don't have knowledge', which might be taken to mean that making predictions about how, and to what extent, China will successfully deal with economic crime in the future is fraught with problems. We should keep in mind the fact that, in the last 30 or so years, no other country in the world has expanded its presence in the global marketplace to the extent that China has. Even Japan's rapid economic growth during the 1960s and 1970s pales by comparison with China's recent advances.

China takes a very severe line on those who transgress and who are caught. The execution of Zheng Xiaoyu, the former Director of State Food and Drug Administration, for economic crimes,

for example, serves as a clear warning to fraudsters. It remains to be seen how foreign investors who fall foul of Chinese economic crimes legislation will be treated.

A recent month-long nationwide amnesty, which resulted in nearly 1,800 Chinese government officials confessing their involvement in hundreds of acts of 'misconduct', serves to demonstrate the prevalence of economic crime and also that China is keen to root it out.

The message is clear. China stands out as a fantastic opportunity for investors, but as the economy continues to grow, so does the opportunity for fraud. Anti-fraud measures that work in Western societies may not be as effective in China, and the need to be vigilant cannot be overstated.

**China stands out as a fantastic opportunity for investors, but as the economy continues to grow, so does the opportunity for fraud**



The background of the slide is a solid blue color with a white grid pattern. The grid consists of vertical and horizontal lines that create a series of rectangular cells. There are several dark, blurry, vertical shapes that appear to be shadows or reflections, possibly of a person's legs, positioned behind the grid. The overall aesthetic is clean and professional.

# Methodologies and acknowledgements

## Methodology

PwC's 4th biennial Global Economic Crime Survey was conducted in 40 countries between April and July 2007. Over 5,400 computer-assisted interviews (telephone and web) were conducted with CEOs, CFOs and other executives who have responsibility for economic crime prevention and detection within their respective companies. More than half of the respondents (55%) are members of the executive board or company management and/or stated that their main responsibility was in the field of finance.

The companies were randomly selected and the target number of respondents for each country was determined according to its GDP.

Each interviewee was asked to respond to the questions with regard to (a) their company and (b) the country in which they are located. The interviews were undertaken in the native language of each country by native speakers, all of whom had been trained in the specific terminology around fraud (see below), as well as fraud's various forms and impact.

Getting these results ready to present to you has taken more than a year, during which we worked to achieve the highest scientific and analytic standards. Work began with a meticulous selection of questions by the international and interdisciplinary members of the project's Survey Management Board. To ensure complete confidentiality of the survey respondents, 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. As a result, all findings have gone through several tests and controls before being released for publication in our survey

The survey also contains a review of the results from 2,026 cases of fraud reported by 1,435 companies. This enabled further, in-depth analysis of its causes and losses, corporate responses and recovery actions and the effectiveness of fraud prevention measures. The survey also contains the opinions of 1568 self-accredited experts on the impact of economic crime in the emerging markets of Brazil, Mexico, China, India, Indonesia, Russia and Turkey.

<b>Western Europe</b>	<b>2550</b>	<b>South &amp; Central America</b>	<b>310</b>
Austria	87	Argentina	76
Belgium	75	Brazil	76
Denmark	75	Chile	76
Finland	80	Mexico	82
France	150	<b>North America</b>	<b>626</b>
Germany	1166	Canada	126
Italy	128	USA	500
Netherlands	150	<b>Asia &amp; Pacific</b>	<b>894</b>
Norway	102	Australia	104
Spain	75	Hong Kong	100
Sweden	76	India	152
Switzerland	84	Indonesia	75
UK	302	Japan	130
<b>Central &amp; Eastern Europe</b>	<b>794</b>	Malaysia	101
Bulgaria	75	New Zealand	78
Czech Republic	79	Singapore	76
Hungary	77	Thailand	78
Poland	102	<b>Africa</b>	<b>254</b>
Romania	77	Egypt	75
Russia	125	Kenya	76
Serbia	76	South Africa	103
Slovakia	78		
Turkey	105	<b>Total</b>	<b>5428</b>

<b>Function (main responsibility) of interviewee in the company (%)</b>	
CEO or Finance	55
Audit	15
Legal	12
Human	8
Security	7
Risk	11
Compliance	11
Other function	27

China experts (resp. for business)	217
China experts (resp. for investment decisions)	313
<b>China experts</b>	<b>530</b>
Brazil	166
India	184
Indonesia	152
Mexico	153
Russia	227
Turkey	156
<b>Total (experts on emerging markets)</b>	<b>1568</b>

Size of participating organisations	
	% companies
Up to 200	34
201 to 1,000	35
1,001 to 5,000	21
More than 5,000	10
Mean number of employees	2842

Industry groups participating	
	% companies
Aerospace & Defence	2
Automotive	5
Chemicals	4
Communication	2
Energy, Utilities & Mining	7
Engineering & Construction	7
Entertainment & Media	3
Financial Services	13
Government Services/Public Services	2
Healthcare	3
Insurance	4
Industrial Manufacturing	15
Pharmaceuticals	3
Retail & Consumer	6
Technology	6
Transportation & Logistics	4
Other Industries or business activities	15

## Definitions of economic crimes

Due to the diverse descriptions of individual types of economic crime in countries' legal statutes, we developed the following categories for the purposes of this survey. The descriptions were read to each of the respondents at the start of the survey to ensure consistency.

### 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 and bribery (inc. racketeering and extortion)

Typically, 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.

## The Editorial Board

The Fourth Global Economic Crime Survey editorial board consisted of the following individuals:

### **PricewaterhouseCoopers Investigations and Forensic Services**

- Claudia Nestler, Partner, Germany Leader and Survey Sponsor
- Steven Skalak, Partner, Global & US Investigations Leader
- John Wilkinson, Partner, Eurofirms Leader
- Tony Parton, Partner, United Kingdom
- John Donker, Partner, Hong Kong/China Leader
- Roger Stanley, Partner, Central & Eastern Europe Leader
- Luis Madasi, Partner, Brazil
- Mona Breed, Managing Director, Global Advisory Client Issues
- Jennifer Johnson, Director, Survey Project Manager

### **Martin-Luther-University (Halle-Wittenberg, Germany)** **[www.econcrime.uni-halle.de](http://www.econcrime.uni-halle.de)**

- Prof. Dr. Kai Bussmann, Chair of Criminology & Penal Law, (Halle/S., Germany)
- Markus Werle, Economy and Crime Research Center (Halle & Berlin, Germany)

### **TNS Emnid (Bielefeld, Germany)** **[www.tns-emnid.com](http://www.tns-emnid.com)**

- Oliver Krieg, Director Social & Opinion

### **Apostasy (London, UK)** **[www.apostasyinnovation.co.uk](http://www.apostasyinnovation.co.uk)**

- Dominic Parker, Strategic Partner, Apostasy Ltd

Particular thanks in compiling this report are also due to the following at PricewaterhouseCoopers: Noel McCarthy, Jennifer Cibinic, Karena Kay.

[pwc.com/crimesurvey](http://pwc.com/crimesurvey)



