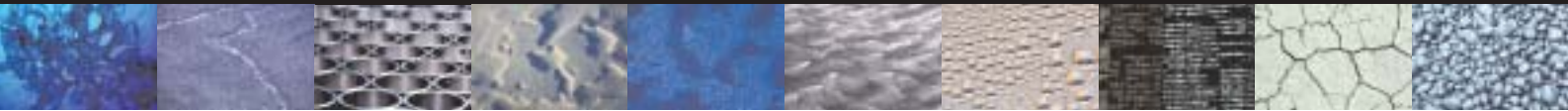


economic crime survey 2003

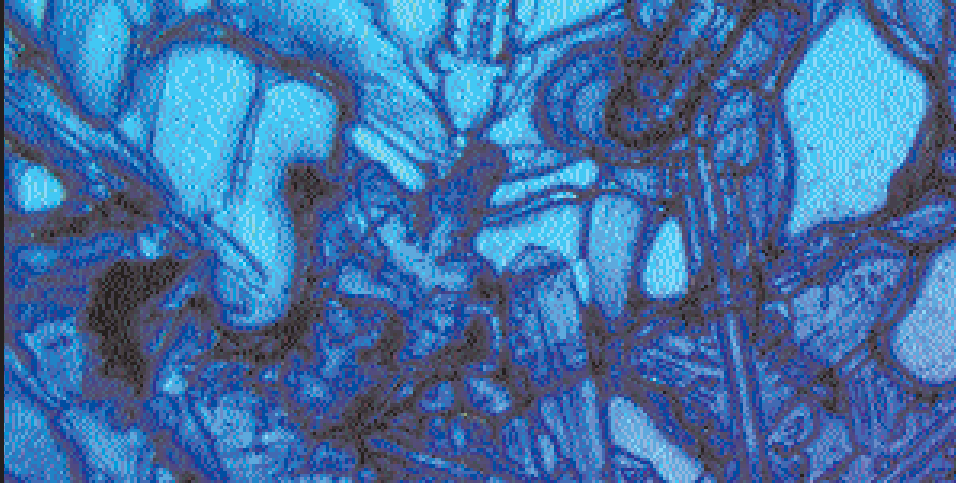
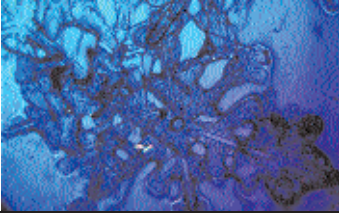


economic crime survey 2003



contents

introduction	2
executive summary	3
economic crime: a growing global threat	4
industries at risk	6
types of economic crime	7
the financial cost of fraud	9
the collateral cost of fraud	10
detecting economic crime	12
managing economic crime	13
recovering stolen assets	14
preventing economic crime	15
economic crime risks of the future	16
survey demographics	18
terminology	19
contact details	20

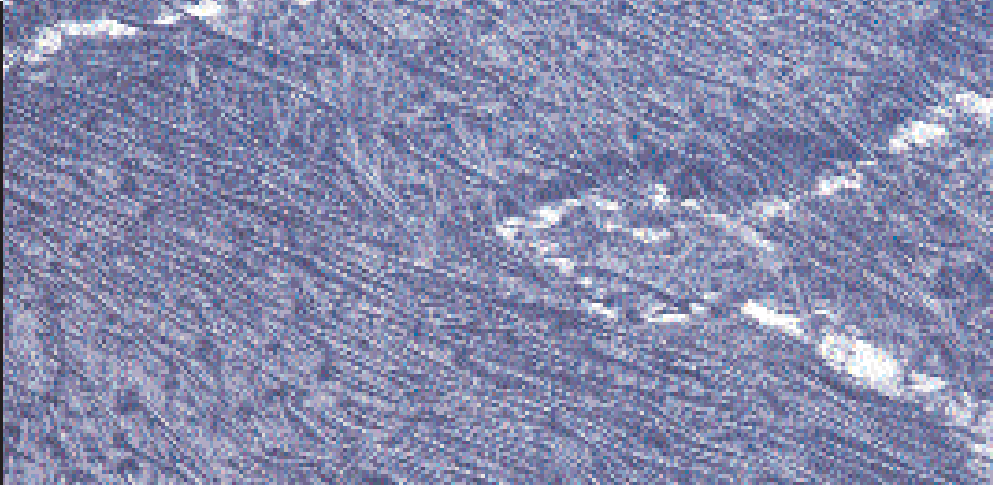


2

introduction

executive summary

- Economic Crime remains a significant threat: 37% of respondents report significant economic crimes during the previous two years.
- The bigger you are, the harder you fall: companies with more employees are more likely to have suffered from economic crime.
- No industry is safe: over 30% of respondents in each of the industries interviewed suffered fraud.
- Asset misappropriation is the most widely reported crime. It is also the easiest crime to detect, with 59% of all victims citing this as one of the frauds that they had suffered.
- Average loss per company: US\$2,252,889
- The impact on reputation, brand image, and staff morale can be more important than the direct financial loss.
- Two-thirds of respondents stressed the company's Board had ultimate responsibility for preventing or managing economic crime – but only just over a quarter had given their boards any risk management training.
- Tangible risk management measures reap clear results: those that had suffered fraud took practical anti-fraud measures, from employee screening to active awareness raising; those that had not, relied on passive measures such as a company code of ethics.
- Three quarters of victims of crime recovered less than 20% of their losses; only half of respondents had insurance against economic crime, but they recovered more of their losses.
- The biggest concerns for the future are asset misappropriation – the most visible of economic crimes – and cybercrime.



economic crime: a growing global threat

Economic crime remains a significant threat to companies across all industries and territories. Well over a third of respondent companies worldwide (37%) said they had suffered from one or more serious frauds during the previous two years.

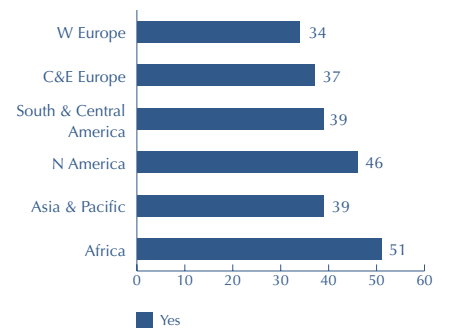
Figure 1: Victims of fraud (worldwide)

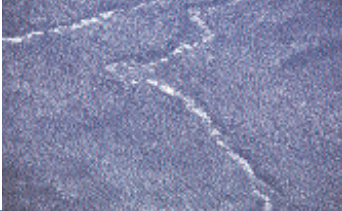
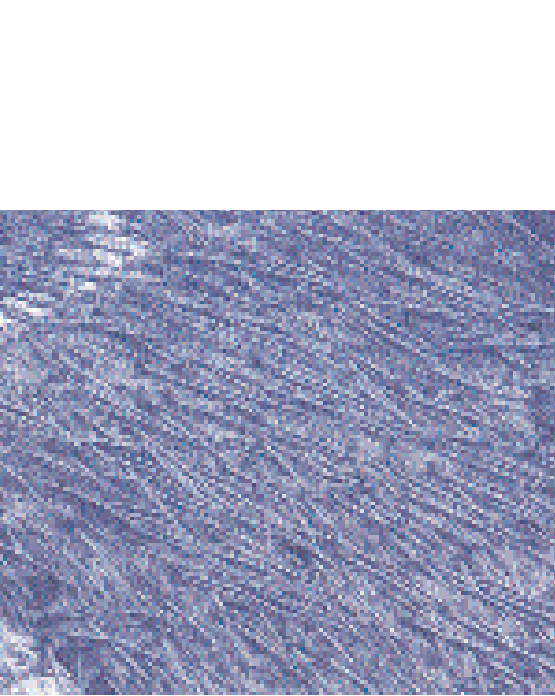
This figure is significantly higher than in our previous European research in 2001. The number of organisations reporting fraud in Western Europe has grown from 29% to 34%, and in Central and Eastern Europe from 26% to 37%. This increase appears to reflect two factors:

- greater awareness of fraud leading to heightened detection rate; and
- a growing desire for transparency, particularly in EU 'accession countries'.

The highest levels of economic crime were reported by respondents in Africa (51%) and North America (46%). In contrast, respondents in Russia and Turkey reported no economic crime at all. There is clearly some way to go in both these countries to either improve detection or to promote greater transparency.

Figure 2: Victims of fraud (by region)



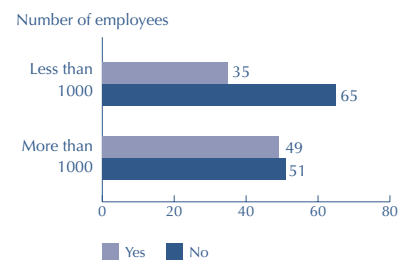


The bigger they are...

Our findings suggest a direct relationship between company size and the likelihood of economic crime. Only 35% of smaller companies (less than 1,000 employees in territory) reported economic crime, compared to 49% in larger companies (over 1,000 employees in territory).

Possible reasons for this higher incidence among larger companies include their greater devolution of operational responsibility, tendency to pursue opportunities in unfamiliar markets, higher transactional complexity, and greater opportunities for collusion amongst employees. Staff in larger corporations may also be less concerned about the financial well being of their employer, regarding fraud as a “victimless crime”.

Figure 3: Victims of fraud by organisation size (worldwide)



Larger companies also generally invest more in fraud risk management systems. This will increase detection rates for most economic crimes.

industries at risk

While all commercial activity is vulnerable to economic crime, its incidence varies between industries.

The results of the Global Survey reinforce our findings from the 2001 European Survey. Financial services (banking, insurance) have reported more incidences of economic crime than other industries. The financial services industry is an obvious target for any fraudster, given the significant quantities

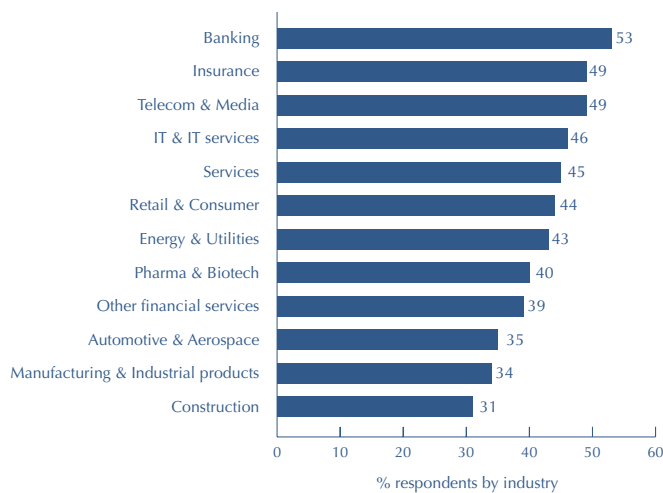
of physical assets held, and access to financial transactions, many of which may be complex.

It is also noteworthy that other highly regulated industries, such as telecoms, appear at the top of this league table. Due to their regulation, these companies have usually developed more sophisticated control and compliance systems. The financial services sector in particular is more

acutely aware of the threat from economic crime. So the higher reported levels of fraud in these sectors partly reflect higher sensitivity to – and detection of – economic crime.

The lower end of the chart contains less regulated industries such as manufacturing and construction. Whilst these industries are prone to economic crimes ranging from asset misappropriation to product piracy, they may often have less sophisticated control and detection mechanisms, or may accept losses through fraud as inevitable.

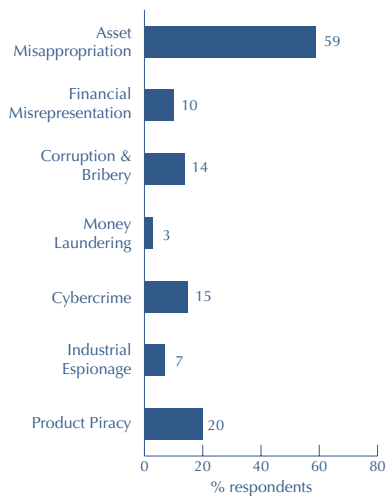
Figure 4: Victims of fraud by industry (worldwide)



types of economic crime

By far the most commonly reported fraud is asset misappropriation, with 59% of those reporting economic crimes claiming this was among them. This type of fraud is generally the easiest to detect, as it involves the theft of tangible items with a defined value. This may help to explain why it is the most commonly reported.

Figure 5: Types of fraud experienced (worldwide)



Perception and reality

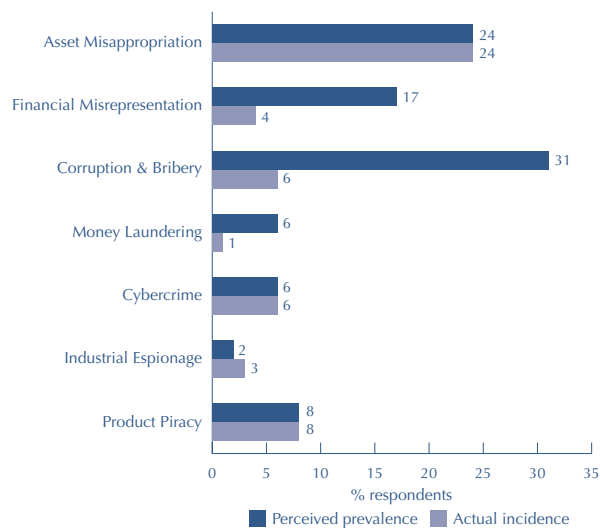
Further insights can be gained by comparing the perceived prevalence of each type of economic crime with its actual incidence.

With asset misappropriation, product piracy and cybercrime, the perceived prevalence and actual incidence are

very similar. This is likely to be due to their greater visibility: lost assets can be counted, counterfeit products seen in the market.

However, with both financial misrepresentation and corruption & bribery, the perceived prevalence is much higher than the reported incidences.

Figure 6: Frauds considered most prevalent compared with their actual incidence (worldwide)

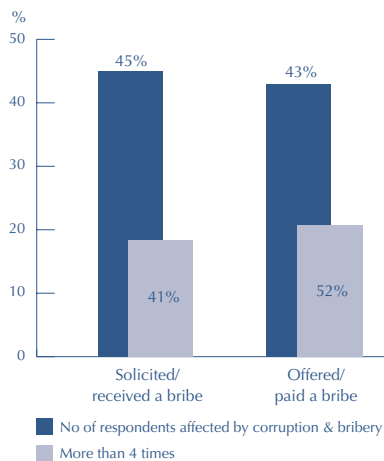




With financial misrepresentation, this gap appears to reflect two factors:

- higher awareness following the corporate scandals in North America and Europe; and
- an understanding that it is likely to have an especially dramatic impact on a business.

Figure 7: Types of corruption & bribery (worldwide)



Given the serious implications of financial misrepresentation, it should be worrying that one in 10 organisations reported incidences (figure 5).

The high perceived prevalence of corruption & bribery reflects the hard work of governments, regulators, and certain NGO's to raise public awareness; an important factor in helping to reduce actual incidence.

199 respondents reported suffering corruption & bribery (worldwide). 45% were solicited with or received a bribe, and 41% of those more than 4 times! 43% were required to offer or pay a bribe – 52% of those more than 4 times! The remaining 12% refused to comment.

The incidence of corruption & bribery has a regional bias towards the developing markets of Africa, South and Central America, and Asia Pacific. In these regions such acts are often viewed as an acceptable element of doing business. Increasing pressure from developed economies is forcing many countries to promote increased awareness of corruption & bribery, and many companies operating in those markets to carefully review their procedures.

It is inevitable that the overall figure for Money Laundering incidence will be low. In order to get a realistic impression of the level or impact of money laundering, it should be assessed according to its incidence within the financial services sector. One in six banks reported having uncovered money laundering during the previous two years. 220 financial services organisations worldwide said they had reported suspicious transactions during the two years, with 20% reporting more than 10 suspicious transactions. This almost certainly reflects the well publicised and ongoing efforts to raise awareness of money laundering and stop movements of illegally obtained funds by convincing countries to adopt internationally accepted anti-money laundering regulations, as well as regularly monitoring their performance.

the financial cost of fraud

We spoke to over 1250 companies that reported losses due to economic crime in the last 2 years. 793 of these companies were able to quantify their loss.

Even when companies know that they have suffered economic crime, they find it difficult to quantify the financial impact on their business. A third of victims cannot even guess how much it cost them. It is clear that the financial cost of less tangible economic crimes, such as bribery & corruption and

cybercrime can be especially hard to quantify. Even with a more quantifiable crime such as asset misappropriation, 21% of victims could not put a figure on their losses.

Among the remaining two thirds (793 companies), we estimate the average loss from fraud was US\$2,252,889.

Figure 8: Financial loss through fraud (worldwide)

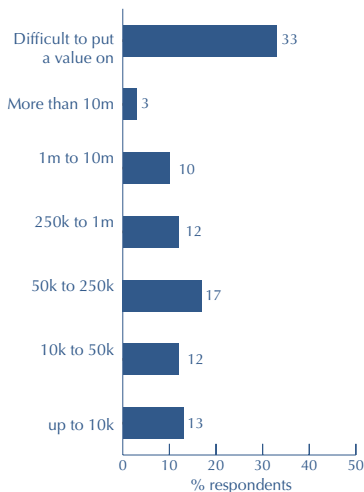
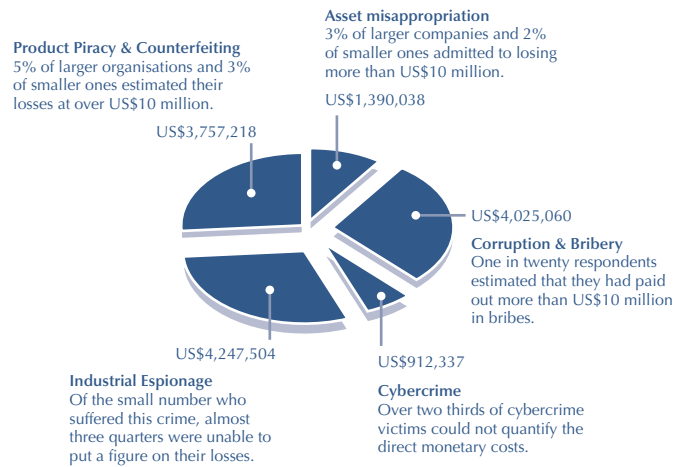
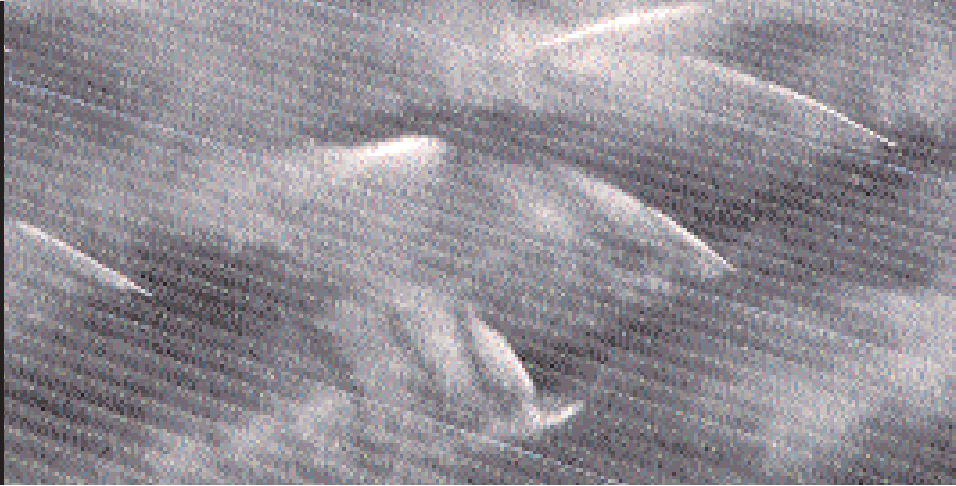
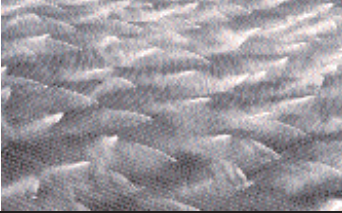


Figure 9: Average financial loss by type of fraud over last two years (worldwide)



The average loss per company from fraud – US \$2,252,889



the collateral cost of fraud

The damage inflicted by economic crime goes far beyond direct monetary loss. Intangible assets including business relationships, staff morale, reputation and branding are critical to any business. These can all be undermined by the occurrence or even the perception of fraud.

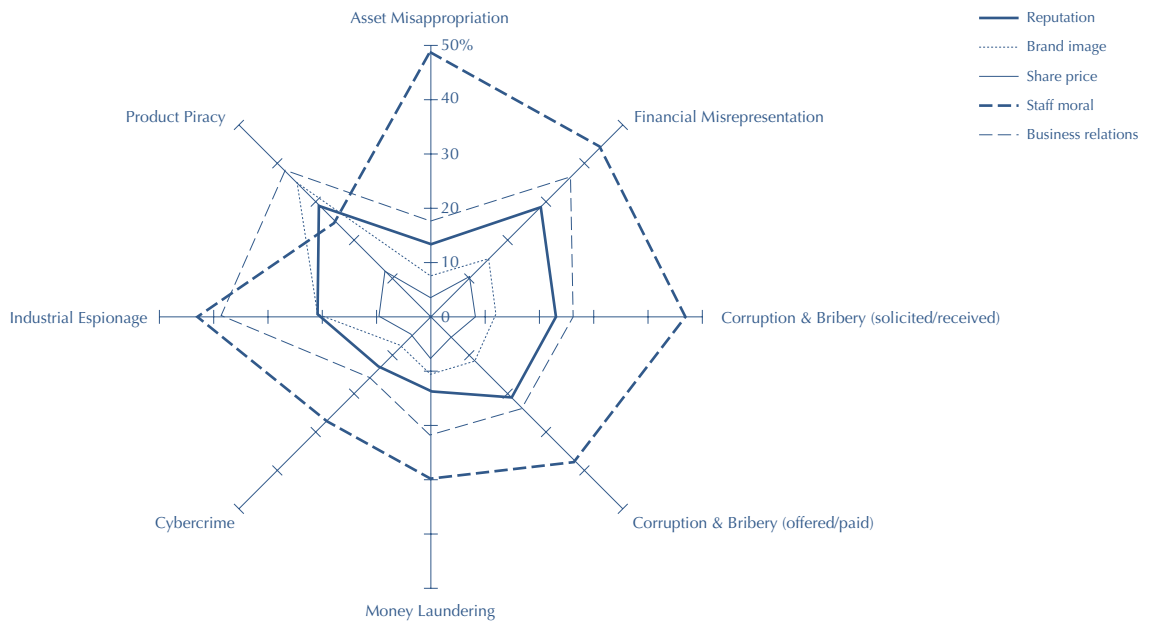
The reported impact varies depending on the nature of the crime committed.

Incidence of economic crime in an organisation invariably raises questions in employee's minds about its leadership and governance, its ethics, or as a secure environment to work. Repeated exposure to such issues can undermine years of carefully built up staff loyalty.

The second most common concern is the effect of economic crime incidence

on external business relationships. It is noteworthy that both asset misappropriation and cybercrime are perceived to inflict less damage in this area than the other forms of economic crime. It may be that organisations accept exposure to these types of crimes as part of the everyday risks of doing business, whereas financial misrepresentation, corruption and

Figure 10: The collateral cost of fraud (worldwide)



bribery may be indicative of wider company issues.

Business relationships and brand image also suffer significantly where product piracy is at play. As a crime extremely prevalent in Africa and Asia Pacific, companies operating in those markets need to be aware of the major impact product piracy can have on product and brand licensing deals by diluting the underlying asset value and creating mistrust among business partners.

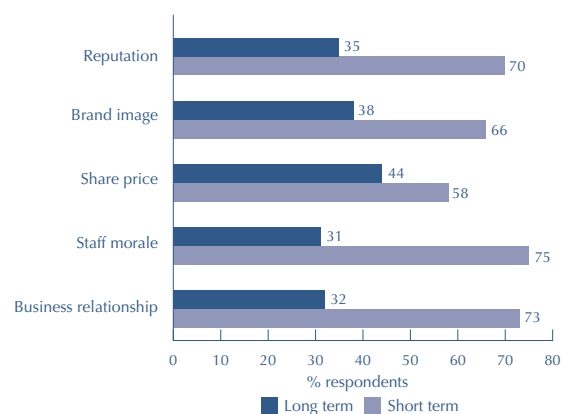
The relationship between economic crime and share performance is a complex issue. A relatively small number of victims felt that fraud had affected their share price – even where financial misrepresentation has potentially called previously disclosed information into question. However, the proportion of respondents who reported an impact on share price as a result of economic crime has doubled since our 2001 research, perhaps indicating that the financial markets no longer view economic crimes as a historical offence with limited future relevance.

Overall, a failure to tackle – or at least manage the risk of – economic crime effectively can store up long-term operational problems for any enterprise. The safeguarding of valuable intangible assets such as brand, client relations, and staff morale should be a key objective.

Asked to consider whether the collateral damage had a short or long-term impact on their business, most respondents

believed the impact to be short-term (less than one year). This should not disguise the fact that approximately one third of respondents reported long-term effects of economic crime on their business, and in the case of share price 44%. A sure sign that collateral damage should be considered on a par with monetary loss when determining economic crime risks.

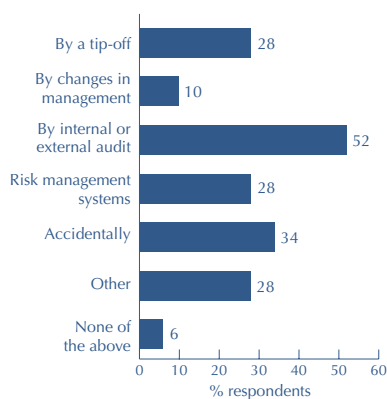
Figure 11: Was the impact of economic crime short or long term? (worldwide)



detecting economic crime

Fraudsters invariably take great pains to conceal or remove evidence of their crimes. As companies can only report crimes that have been detected, it is not possible to judge how much fraud goes unnoticed. What we can analyse is the means by which fraud is brought to light.

Figure 12: How economic crime is detected (worldwide)



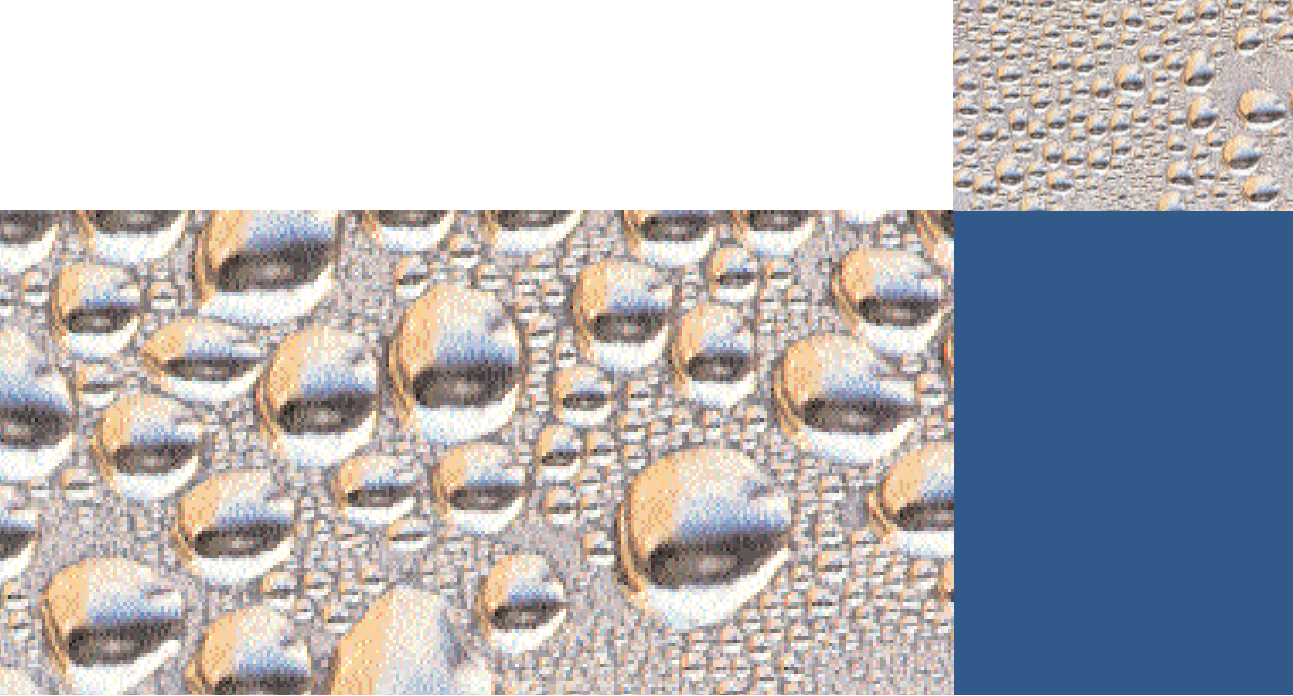
The results vary considerably depending on the size of the organisation concerned. Within larger organisations a combination of factors are likely to be involved in the detection of an incident. Large companies most often detected fraud through their control and risk management systems. However, in many cases this was accompanied by a finding from the internal or external audit function or from a tip-off.

Smaller organisations detected a far greater proportion of economic crime through audit processes than by other means. Given the respective size of the organisations this is most likely to be via the external auditors – a worrying finding that suggests smaller companies may be placing too little attention on the development of effective controls and alternative checks and balances. Over-reliance on a single annual review to root out problems may be playing into the fraudster’s hands.

A consistent theme from our previous European survey is that over a third of economic crimes at major companies are uncovered by accident.

Clearly, reliance on luck is not a basis for an anti-fraud regime. However, even where companies have control systems to detect economic crime, these can often be rendered ineffective by management override or collusion. Companies need to do more in terms of:

- Assessing the real risks and vulnerabilities to fraud within the organisation
- Communicating actively the company’s stance on fraud and “walking the talk”
- Proactively monitoring risky areas
- Developing policies to encourage (and protect) “whistleblowers”
- Expecting the worst and being prepared – devising a robust fraud response plan

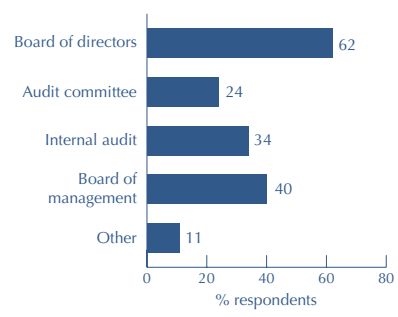


managing economic crime

Respondents assign primary responsibility for managing economic crime issues to the board of directors. 62% of respondents stated that the board must be informed of all instances of economic crime. There are significant regional variations however. Within Asia & Pacific (83%) the responsibility is vested firmly with the Board. Significantly fewer companies in North America (45%) and Central & Eastern Europe (47%) rely on the Board to fulfill this duty. In both these regions, company management is just as likely to have responsibility for managing the issues.

Regardless of where the primary responsibility lies it is surprising that only 28% of organisations have implemented any fraud-related training for the Board or management. Given the increasing focus on corporate fraud with regulators, ratings agencies and others now scrutinising companies for signs of misdeed, Boards and management need to consider making this type of training part of their corporate governance regime.

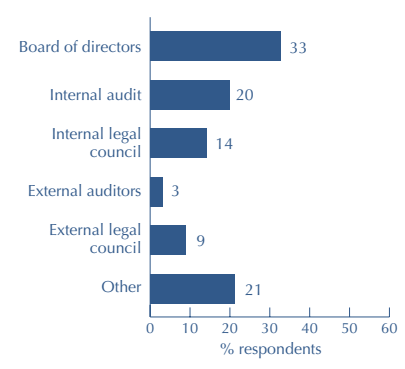
Figure 13: Bodies to which economic crime must be reported (worldwide)



Respondents' opinions varied on how economic crimes should be dealt with once detected. Overall 63% of respondent organisations said they had a requirement to report frauds to an external body. Once more though, regional variations are significant. In the Asia & Pacific region only 48% of companies had a requirement to involve the authorities. In Africa and Central & Eastern Europe over 80% of companies said that they applied this policy.

We are surprised that this figure is so high. Our experience in investigating economic crime for corporations suggests that there are many reasons why an organisation may choose not to report a fraud to an external body. These include the potential impact of negative publicity on business relationships or staff morale. In addition, companies often fear the costs of a drawn-out judicial process, or simply believe there is little chance of recovering the stolen assets. It may well be that companies have a public face supporting a policy of reporting all matters to the authorities, but become more pragmatic when faced with an actual event.

Figure 14: Responsibility for dealing with economic crime (worldwide)



recovering stolen assets

Even if economic crime is detected and prosecuted, it can still prove impossible to recover the assets. Of respondents who had experienced fraud, only 8% had succeeded in recovering more than 80% of their losses, whilst almost three-quarters recovered less than 20%.

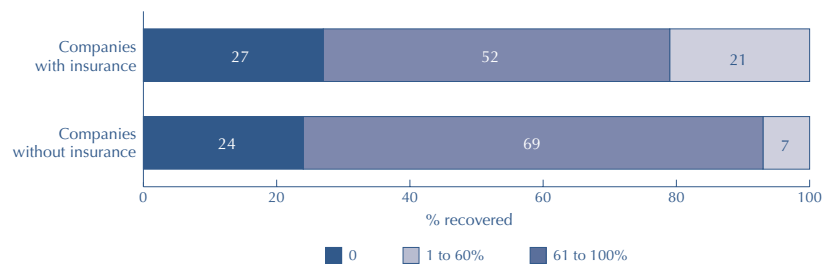
There are many reasons for this relative failure to recover lost assets. Companies are reluctant to embark on long recovery processes with no certainty of success, especially where the assets have been moved across borders. However, there may be good reasons to pursue the assets regardless – firstly 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 to create the right culture of deterrence.

Insurance

Surprisingly, given the high awareness of economic crime, less than half the organisations surveyed had taken out insurance against fraud losses. This may be due to management indifference or scepticism over how much insurance could actually recover.

However, insurance can have a significant impact on recoveries. Companies with insurance reported being 300% more likely to recover more than 60% of their losses.

Figure 15: Recoveries of companies with and without insurance (worldwide).



preventing economic crime

Not surprisingly, companies that have suffered economic crime are more concerned about the strength and effectiveness of their systems to prevent fraud. They are also more likely to have taken proactive measures to reduce future exposure.

Our findings illustrate the impact of fraud on an organisation’s mindset.

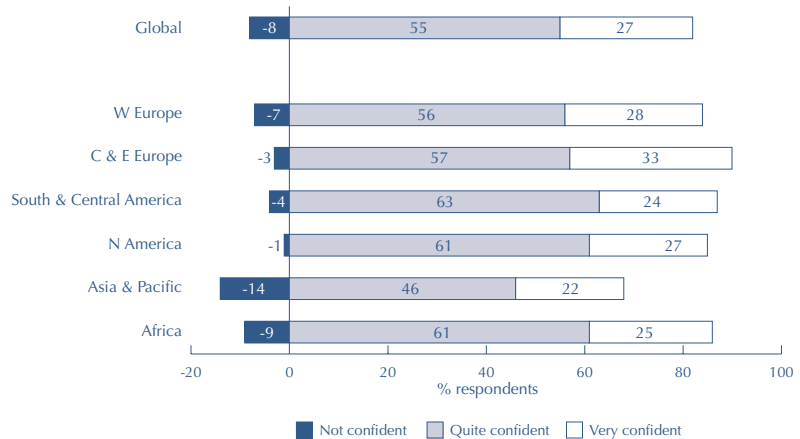
Those that had not suffered fraud tended to rely on more intangible prevention tools such as codes of conduct or ethical policies. In contrast, fraud victims instituted more tangible measures such as employee screening, management training and whistleblowing programmes. They also invested greater effort in raising awareness of the potential for economic crimes.

Organisations that take practical measures to combat fraud, and that effect change on the ground rather than creating the appearance of addressing the problem, will develop a stronger culture of prevention. As a result of such action, companies that had reported economic crime are “quite” or “very” confident that their anti-fraud controls are stronger now than they were two years ago.

Figure 16: Types of corrective measures taken (worldwide)



Figure 17: Confidence in fraud risk management systems



economic crime risks of the future

Most organisations expect the threat of economic crime to increase over the next five years, with respondents in North America and Africa being especially pessimistic. Our findings support this general perception that the risk will increase.

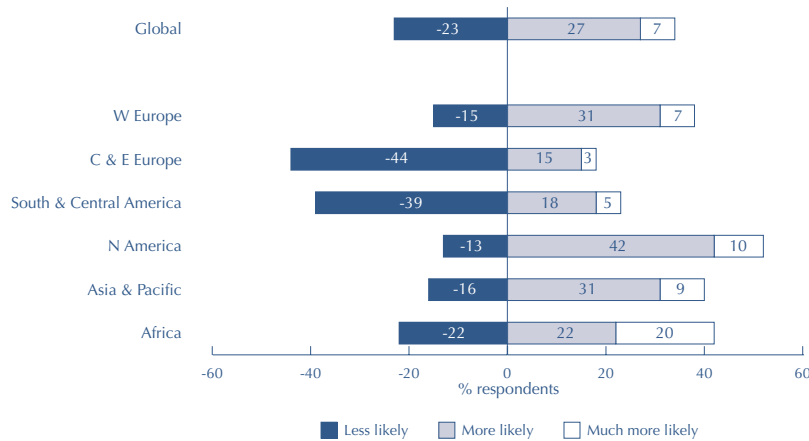
However, companies in Central & Eastern Europe and South & Central America expect the risk to decrease.

The responses from Central & Eastern Europe are in line with our European survey of 2001. Then companies surveyed also showed some optimism for a fall in economic crime risks in that region. In the last two years however, our respondents in Central & Eastern Europe reported significantly more economic crime (2003: 37%, 2001: 26%). In our view it is unrealistic to expect decreases in economic crime

risks without substantial actions to tackle the roots of all economic crime: motive, opportunity and a clearly perceived benefit of reward over punishment.

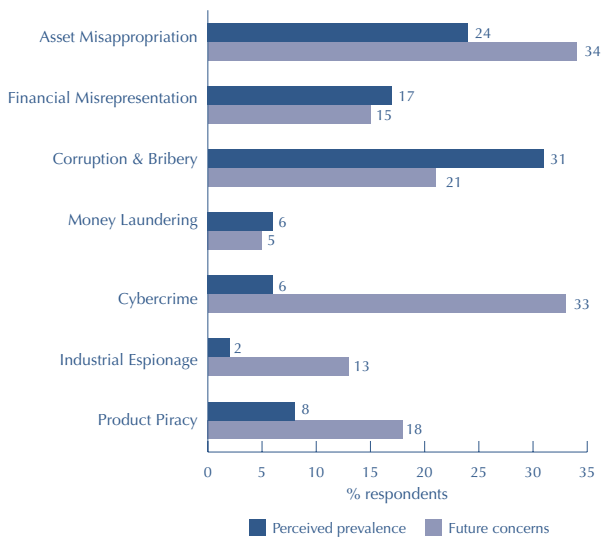
Looking forward over the next five years, 34% of companies expect their greatest economic crime risk to be asset misappropriation – currently the most frequent form of fraud worldwide – and 33% cybercrime.

Figure 18: Expectation as to whether fraud risk will increase over the next 5 years



Compared to our previous European survey where cybercrime was by far the greatest fear for the future (2001:43%) this is a significant decrease. Regional factors do play a role however in this analysis. Asset misappropriation is most noticeably seen as a threat in Africa (48%) and North America (52%). In the Asia & Pacific region however, cybercrime is still seen as the key risk for the future with 35% of companies citing this as their chief concern. 27% of South and Central America companies agreed with them, however a similar proportion believe that the issues of corruption & bribery will remain their greatest economic crime threat.

Figure 19: Frauds considered most prevalent compared with future concerns (worldwide)



The lower proportion of respondents anticipating cybercrime as the most significant future threat (figure 19) may reflect two factors. Firstly, much activity initially categorised as cybercrime was in fact 'traditional' fraud conducted by electronic means – for instance, asset misappropriation through tampering with payment data – rather than crimes now clearly defined as cybercrime such as denial of service attacks, theft of

electronic data and the use of viruses. Companies now define cybercrime more accurately, and expect fewer occurrences as a result. Secondly, whilst the effects of cybercrime can be extremely severe for those companies targeted, it appears that many cyber criminals are extremely selective in their targets. Companies that have not yet been made a target may be breathing a premature sigh of relief.

survey demographics

This survey was the result of 3,400 interviews in 50 countries. The number of interviews conducted per country was:

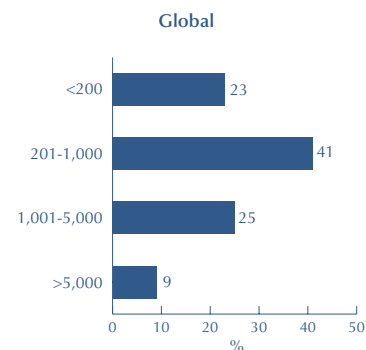
Western Europe	1476	South & Central America	554
UK/NI/ROI	162	Argentina	96
Austria	83	Brazil	86
France	156	Chile	53
Germany	150	Columbia	48
Norway	90	Dominican Republic	31
Portugal	50	Mexico	87
Spain	106	Guatemala	30
Sweden	91	Peru	51
Switzerland	89	Uruguay	36
The Netherlands	103	Venezuela	36
Italy	159		
Denmark	88	North America	103
Greece	59	Canada	103
Belgium	90	USA	
Central & Eastern Europe	378	Asia & Pacific	878
Czech Republic	50	Australia	100
Estonia/Lithuania/Latvia	25	Hong Kong	85
Hungary	25	India	85
Bulgaria	25	Indonesia	85
Poland	85	Japan	423*
Romania	29	Singapore	50
Slovenia	27	Thailand	50
Turkey	52		
Russia	29	Africa	143
Slovak Republic	31	Algeria	21
		Morocco	17
		South Africa	91
		Tunisia	14

*weighted in the statistics to reflect a base of 150 respondents

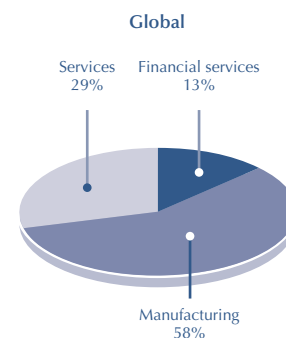
Percentages may total more or less than 100 per cent as respondents were able to provide multiple answers or may have chosen not to answer.

8 companies suffered economic crimes totalling in excess of US\$100 million, and have been removed from the "total cost" analysis.

The size of participating organisations was as follows:



Respondents were CEOs and CFOs and those responsible for preventing and detecting fraud. They were drawn from the following industry sectors:



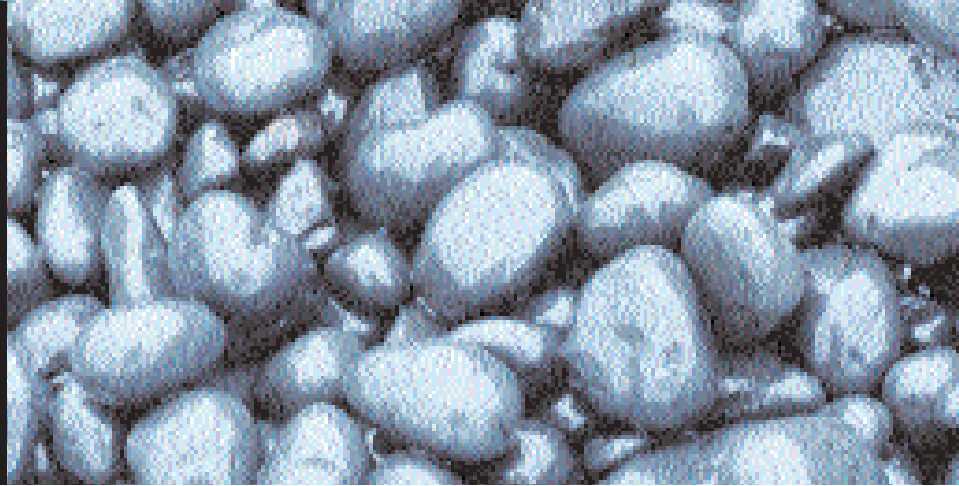
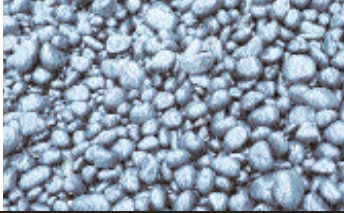
terminology

Due to diverse descriptions of individual types of economic crime in countries' legal statutes, we have developed the following categories for the purposes of this survey. The descriptions were read to each of the respondents at the start of each 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 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.
Financial misrepresentation	Company accounts are altered or presented in such a way that they do not reflect the true value or financial activities of the company.
Corruption & Bribery (inc. racketeering & 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.
Cybercrime (e.g. hacking, virus attacks, denial of service, electronic theft of proprietary information)	The illegal access to a computer or computer network to cause damage or theft.
Industrial espionage & information brokerage	The acquiring of trade secrets or company information by secretive and illegal means and/or the selling of these secrets or information to interested parties.
Product Piracy/Counterfeiting	The illegal copying and/or distribution of fake branded goods in breach of patent or copyright. This also includes the creation of false currency notes & coins with the intention of passing them off as genuine.

Other terms used in the survey

Whistleblowing	The disclosure by an employee of malpractice in the workplace
Tip-off	A hint or indication about goings-on in the organisation
Audit	The formal examination and review of a company's accounts and/ or practices.
Risk management systems	Systems put in place to assess, identify and respond to risks in the company.
Soliciting or receiving a commission	Being offered or given money or other incentives to help influence a business decision in the donor's favour.
Offering or paying a commission	Having to offer or give money or other incentives to help influence a business decision in your favour.



contact details

endnotes

¹ The majority of companies would have found it a near impossibility to quantify exactly the financial impact of a fraud or frauds upon them. In order to facilitate their answering of this question, we provided a series of financial ranges for them to work within:

- < US\$ 10,000
- US\$ 10,000 – 50,000
- US\$ 50,000 – 100,000
- US\$ 100,000 – 250,000
- US\$ 250,000 – 500,000
- US\$ 500,000 – 1 million
- US\$ 1 million – 5 million
- US\$ 5 million – 10 million
- US\$ 10 million – 50 million
- US\$ 50 million – 100 million
- > US\$ 100 million

The values quoted in the report are estimates derived from a computation that assigned a midpoint to each value range for the frauds which a company reported it had been subject to. This provided a total cost of fraud for each individual company from which was calculated (1) the average figure and (2) the total figure.



