Developing effective tools to manage the risk of damage caused by corporate fraud and management misconduct

Rosalind Wright CB
Chair, Fraud Advisory Panel
London, UK

Outline:

1. What is corporate fraud?
   - fraud committed on an organisation by an external agency
   - fraud committed on an organisation from within
   - fraud committed by an organisation on others

2. Size of corporate fraud: what is the impact on business?

3. Typology of offences:
   - piracy and copyright theft
   - Identity fraud
   - theft by employees or directors (Barings, Maxwell); breach of fiduciary duty
   - false accounting (Enron, WorldCom)
   - corruption
   - phoenix companies
   - long-firm fraud

4. Effects of corporate fraud
   - on the business itself as direct victim
   - on the business sector
   - reputation of financial centre

5. Tools to combat corporate fraud
   - By law enforcement;
     - Legislation (Fraud Bill, corruption legislation including Terrorism, Crime and Police Act for overseas corruption)
     - Law enforcement powers
       - Arrest, investigate and prosecute
       - Restitution
       - Asset recovery
       -
   - By industry

- Recognition that fraud is a business risk
- Inclusion of it in risk assessment and at strategy planning level
- Planning an anti-fraud policy, including attitude to whistle-blowing
- Disseminate anti-fraud Statement to staff and directors
- Ensure that it is working – assign responsibilities
- Illustrate anti-fraud Policy statements
- Institute ethical culture within organisations.

Introduction

Fraud has to be taken seriously. It costs the UK economy alone an estimated £14bn a year: £230 for every person in the UK. It facilitates other crime, such as terrorism. There is clear evidence that it is becoming a crime of choice for organised crime and terrorist funding. The response from law enforcement world-wide has not been sufficient. We need to bear down on fraud; to make sure that laws, procedures and resources devoted to combating fraud are fit for the modern age so we can tackle sophisticated economic crime vigorously and effectively. But industry and business has much to do to protect itself from the threat of fraud.

In this talk, I want to address the impact fraud has on business and the economies of the world; to highlight the threat of financial crime which is hitting all of us here today; and to demonstrate that there is much that corporations and organisations can do to tackle the threat of fraud and its impact.

What is corporate fraud?

Fraud can be perpetrated on organisation both from outside – the external threat – and from within. Organisations can be set up for the principal purpose of defrauding others and, using the agency of a limited company; fraudsters can perpetrate serious economic offences shielding themselves behind the veil of incorporation. Large-scale corporate fraud can have devastating effects. We have only to look at Enron (losses estimated at $1.5 billion), WorldCom ($3.8 billion) Barings £827 million ($1.4 billion) to see the impact that corporate dishonesty and misconduct can have on a business. Shareholders and bondholders lost everything; thousands of employees and pensioners lost their jobs and their future financial security.

This is only half the picture, however. The real impact is felt much more deeply than in the business itself. We must take into the equation the effect on the credibility of the sector in which the affected business operated; the effect on market confidence and on the reputation of the financial centres in which the business was done. This is an unseen and largely unquantifiable loss but a very real on, nevertheless.

Let us examine for a moment, the extent to which corporate fraud is perpetrated. PricewaterhouseCoopers carried out a global survey of 3,600 corporate executives in 34 countries in 2005, which reported that -

- 45% of companies had fallen victim to fraud in the past two years
- On average they recorded suffering an average of 8 serious incidents each
- Since 2003 there has been:

    - a 71% increase in the number of companies reporting cases of corruption & bribery
    - a 133% increase in the number reporting money laundering; and
    - a 140% increase in the number reporting financial misrepresentation

- Fraud that led to a loss of assets cost companies—on average—over US$ 1.7 million: a 50% increase over 2003
- 40% of suffered significant loss of reputation, decreased staff motivation, and damaged business relations
- Over one third of these frauds were discovered by accident, making "chance" the most common fraud detection tool.

Fraud is now the crime of choice of organised criminal gangs worldwide. The likely gains are enormous and the likelihood of apprehension and thus of conviction and punishment comparatively small compared with conventional crimes of dishonesty involving guns, intimidation and violence of all kinds. Professional criminals are targeting big business. The notorious bank robber, Willie Sutton, used to say he robbed banks because that's where the money is. So it is with organised crime, and how better to attack a corporation and get to its assets than by corrupting its employees, by planting its own men within an organisation to get hold of confidential data and rob it from the inside?

Fraud targeted at a business almost invariably has links within the business. The few instances of crime that are aimed wholly from outside are now confined to computer crime, such as denial of service attacks (a form of blackmail, where a business, usually a small or medium size enterprise) is bombarded with emails until its systems crash. Demands are then made, often repeatedly for money to stop the attack.

Other forms of external attacks on business come in the form of copyright theft or commercial piracy. Companies lose millions through the unauthorised copying and selling of copycat products, which can range from fake plastic Gucci handbags to antibiotics and aircraft parts. Nobody ever died of a fake fashion accessory, but children throughout the third world are put at is of certain death from fake drugs which are largely inert substances, often talcum powder and aircraft have dramatically and inexplicably fallen out of the skies when fake bolts have failed.

Identity theft aimed at companies is not a new phenomenon. Company identity fraud is similar to personal identity theft. It is surprisingly easy to change company documentation. Without a great deal of knowledge or effort, a fraudster can change the registered office, trading address, and even the names of directors of a company without the company's knowledge. In the UK, Companies House have to accept documentation it receives at face value, so any checks that are undertaken on the cloned company will show that the applying director is an official director of the company and that the address given is the Registered Office of the company. In

addition, any ordinary credit search against the business with any of the credit reference agencies is likely to show a healthy credit rating, hence there will seemingly be no reason not to accept the order.

Once the company's address is changed, the fraudsters can order goods from current or new suppliers in the company's name to be sent to the new address. Any supplier carrying out a check on the details kept at Companies House will be unaware of any criminal activity and using the company's own well-established credit rating will dispatch goods to the fake address.

There will always be at least two direct victims of corporate ID fraud. The company whose details are taken and any other undertaking that then supplies goods or services to the cloned company. And ultimately everyone pays for this fraud indirectly through higher product costs and insurance premiums.

Smaller companies can sometimes fall prey to advance fee fraudsters, those credible conmen who can persuade even sophisticated businesspeople that they would like to invest in their companies, but a small "administration" fee or even a kickback is necessary to set the ball rolling. Charities have succumbed to this form of fraud which is more commonly seen targeting individual victims, but even the UK's National Coal Board, in a famous attempted con, back in the 1980s, has fallen prey to the blandishments of the silken-tongued conman. A variation on the theme is the crooked financial institution set up to offer fictitious finance to individual or companies who are unable to obtain finance at an affordable rate elsewhere; again for a small upfront fee, usually a percentage of the fiancé offered, the fraudsters persuade the victim to part with often sizeable sums of money. In one case prosecuted by the SFO in the 1990s, a phoney bank was set up in Torquay, in Devon, UK, by three international crooks, to persuade property developers and builders to part with advance fees to secure finance for building projects in Germany and Austria. Needless to say, once the advance frees were secured, the finance and the fraudsters vanished into thin air.

Insider fraud can do the most damage however. Theft or financial manipulation by staff and directors is the commonest form of fraud experienced by companies. The PwC survey found that asset misappropriation by employees, generally the easiest fraud to detect as it involves the theft of tangible assets with a defined value, is the single most common form of economic crime affecting 82% of those businesses which fell victim to fraud. UK companies reported a higher level of asset misappropriation than elsewhere in the world and it appears that insufficient attention is being paid in the UK to a form of economic crime which is generally considered to be easier to prevent.

Looking to the future, 49% of companies expect fraud to increase in the next five years and 52% of companies expect their greatest fraud risk to continue to be asset misappropriation, followed closely by cybercrime (48%).

Instances of employee fraud are so well known that it otiose to list them – but my audience will instantly bring to mind such notorious examples as Nick Leeson at Barings, Joseph Jett at Kidder Peabody and even Joyti de Laurey, a secretary at Goldman Sachs in London, who stole £4.3 million ($7.7 million) from her line

manager and his wife's bank accounts to fund her own lavish lifestyle. Robert Maxwell, the press baron and former MP who drowned in the Mediterranean in October, 1991, left a trail of creditors and pensioners in his wake, whose money he had plundered from his own company's pension fund.

Directors are no less likely to rob their own corporations than the more lowly members of staff. Opportunity and motive, often heavy indebtedness, strike the finance director or even the chief executive as often as the secretaries and the clerical staff. Breach of fiduciary duty by professional men and women is a recognised element of financial misconduct and treated particularly severely by courts and regulators. Protiviti, the independent risk consultants, recently carried out a survey of convicted fraudsters, many of them employee or directors who had plundered their own companies. One fraud commonly committed by employees is the drafting of phony invoices and transfer of funds.

They found the common theme among all of them was debt. In many cases, they were previously honest and hard-working members of staff who were dragged into a world of corporate fraud by financial problems - which ranged from "an expensive wife" or private school fees for their children to more common debt problems such as gambling or credit and mortgage repayments.

However, the incredible ease with which they were able to carry out their crimes and the fact their activities remained undetected for some time meant many were unable to stop stealing from their companies once they had cleared their debts – especially as they grew accustomed to their 'extra income'.

Protiviti comments: "The problem with corporate fraud is that the people doing this are experts in their field. They know their companies inside out. They know the computer systems and they know exactly what to do."

The failure of companies to demonstrate a hard line on fraud and control the problem created added temptation for staff convinced they would get away with their crimes.

A recent and worrying development is the infiltration of companies and financial houses, such as banks and building societies (mutual funds) by criminals, intent on gaining access to confidential customer information. They then sell the details to other criminal gangs, or use it themselves to rob customers' accounts. Bank employees are continually targeted by criminal gangs, so much so, that many banks have forbidden their employee from wearing distinctive bank uniform or identity badges outside the office, for fear of being picked out by talent scouts for criminal gangs, offering them inducements to betray confidential information.

Companies set up deliberately to defraud the public or other business are comparatively rare. But the corporate identity and its limited liability protections for directors are an irresistible lure for the dishonest businessman or woman.

An example of a company formed to defraud others is the long-firm fraud. An apparently legitimate business is set up and develops a respectable credit history to win the trust of suppliers; by placing numerous small orders with wholesalers and ensuring they pay promptly. When the fraudsters are ready, they place several larger

orders with the businesses with which they have established a good credit history. Once they receive the goods, the criminals will promptly disappear and sell the goods on from various trading places. Most long firm frauds are set up with the intention of carrying out the fraud within a year or two. This means they can disappear before they have to file any accounts at Companies House.

A further example of a company set up to fail is the phoenix company. A director or directors set up a business, and then winds it up owing substantial amounts of money. The directors then create another company, operating in the same field, often using a similar or even the same company name. Creditors of the original company lose out when the company goes into liquidation. The directors have no financial responsibility to settle the debts – yet they can start up again with no negative impact.

The effects of corporate fraud

The risks of fraud within and upon corporations cannot be understated. They include the immediate risks to the company affected, which can fail completely, like the huge US giants and Barings Bank, the oldest independent investment bank in the UK. There is also the reputation risk to the company that has suffered major fraud. This is one reason that companies and particularly financial houses are so reluctant to report fraud to law enforcement, where they fear that the likelihood of their names hitting the headlines associated with major losses will result in competitors' obtaining an advantage and customers walking away. Systemic risk, that affects an entire financial market or system, and not just specific participants, cannot be underestimated. After the secondary banking crisis in the 1980s, where so many minor financial houses failed, largely as a result of fraud, confidence in the banking sector was shaken severely.

What can law enforcement do to tackle the problem of corporate fraud?

There are two aspects to effective law enforcement in this area: firstly, the legislative tools to do the job; and secondly, the resources to ensure that the job can be done.

Legislation

In the UK, we are just about to bring into law the Fraud Bill, which will make enormous changes to the way that fraud is charged and prosecuted in the UK.

The current law on fraud in England and Wales is fragmented, disparate and overspecific. It is made up of several common law offences and numerous statutory offences found in various Theft Acts passed between 1968 and 1996. It is a peculiarity of our law that it knows no specific offence of fraud. Instead we have statutory offences of deception, which are too precise, overlapping and outmoded to give effective coverage over the breadth of frauds committed today.

The Fraud Bill was introduced into Parliament in May 2005, and is the culmination of a lengthy process of careful consideration, including a 2002 Law Commission Report and wide consultation. The Bill will replace the existing offences of deception in our Theft Acts with a general offence of fraud which can be committed in several defined ways. It aims to provide a clear and robust legal framework which is flexible enough

to deal with increasingly sophisticated and modern types of fraud. The Bill has wide support from investigators, prosecutors and other stakeholders and consultees, such as the banks and those concerned with copyright and piracy.

It also received wide support from the members of the House of Lords when the Bill was introduced. Indeed the only real disagreement on the substance of the Bill is that some think the Bill does not go far enough and we should take the opportunity to repeal our common law offence of conspiracy to defraud. But on the advice of Investigators and prosecutors, who have argued that the availability of this offence is crucial to the prosecution of the most sophisticated frauds that repeal has been successfully resisted. There could be great difficulty otherwise in prosecuting a number of cases such as large scale credit card frauds where a number of people are involved in different aspects of the scheme. Indeed, the senior judiciary have said that they regard the conspiracy charge as the most effective charge where multiple defendants are engaged in a fraudulent course of conduct, and that it would risky to repeal it.

Secondly reforms to the law of corruption have been made and are still under discussion. Corruption is potentially devastating. If it is not kept in check, it has the potential to cause serious damage to government and business – indeed to every aspect of economic and social life. Corruption is a complex crime, by its very nature insidious and its effects stretch across international borders. Corruption world-wide weakens democracy, harms economies, impedes sustainable development and can undermine respect for human rights by supporting corrupt governments, with widespread destabilising consequences.

The Anti-terrorism, Crime and Security Act 2001 has made the offering of a bribe to officials outside the UK by a national of the United Kingdom or a body incorporated under the law of any part of the United Kingdom an offence on the same basis as the prevention of Corruption Acts, which relate to bribes paid or received within the UK. So far, there have been no prosecutions for this offence but I know this is a topic which will be covered in depth later ion during this conference, so I will leave others to discuss the problem and difficulties of mounting a criminal investigation for an offence where the actus reus and most of the evidence will be abroad and have to be adduced in an English criminal court.

The UK Government introduced its Corruption Bill in 2003 in the context of a multi-faceted strategy to tackle corruption both at home and internationally.
Existing corruption law, drawn from a range of sources from as far back as 1889, is outdated. In its 1998 report, the Law Commission describes it as “obscure, complex, inconsistent and insufficiently comprehensive”. It can be difficult for our law enforcement authorities to use and the inconsistency, lack of definition and various lacunae might lead to corrupt individuals’ being acquitted. It shies away from the most important question – it does not have a definition of what acting corruptly actually means. The Bill is drafted on the basis of a Law Commission report. It modernises the law by bringing together all offences of corruption in a single statute and addressing existing lacunae. It defines what is meant by “acting corruptly” and ensures that the law on corruption applies equally to all. Following the recommendation of the Joint Committee on Parliamentary Privilege of June 1999, in the event of a corruption prosecution, MPs and Peers will no longer be subject to the

protection of parliamentary privilege – under which evidence of proceedings in Parliament is not admissible in court. In addition, the Bill amends civil law to enable ratification of the Council of Europe Civil Law Convention on Corruption, which aims to ensure that those who have suffered damage as a result of acts of corruption are able to defend their rights and interests. The Bill has yet to be enacted.

The resources

It is widely accepted that most investigating and prosecuting authorities suffer from inadequate funding and manpower. There are many bodies responsible for the investigation and/or prosecution of frauds, for example the SFO, the Crown Prosecution Service ("CPS"), the Revenue and Customs Prosecuting Office ("RCPO"), the Department of Trade and Industry ("DTI"), and the Financial Services Authority ("FSA") but, it is thought, too few investigators to assist in what are frequently mammoth investigations and lengthy and detailed exercises in marshalling information for a prosecution. In fact, although the SFO is the one body that exists purely for the investigation and prosecution of large and complex frauds, it deals with only a small number of frauds. The CPS prosecutes a significant proportion of the total number of fraud cases, yet as a body its focus is not on this area, but rather on prosecuting generally. The remaining prosecuting authorities, such as the DTI and FSA, have more limited resources than either the SFO or CPS. Indeed it is common for other authorities to begin an investigation into a suspected fraud, only to find that it is serious or complex so that responsibility will fall on the SFO. This system gives rise to further delays, and can, for example, interfere with the later prosecution by the SFO where the original prosecuting authority has elicited confessions under compulsory powers, which cannot then be used at trial.

The Fraud Advisory Panel noted in its annual review for 2003-4 that the Commissioner of Police for the City of London had commented that police forces had been distancing themselves from fraud investigations for years. There were 869 mainstream fraud investigators in 1995, compared with around 600 some nine years later.

Without adequate police resourcing for fraud – and this is not a problem confined to the UK – major criminal fraud will go uninvestigated.

It is reassuring that the newly formed Serious Organised Crime Agency, set up to tackle criminal gangs involved in the most serious of criminal offence, will have non-fiscal fraud as one of its major priorities. The CPS will itself be resourced to prosecute major organised crime and, it is hoped, have its fraud prosecuting function, which has been sadly depleted and dissipated over recent years, restored to something approaching an effective resource to prosecute cases of major fraud which are not tackled by the SFO.

What can industry and business itself do to tackle the threat of fraud?

First, it should recognise the threat of fraud as a business risk and a very real and substantial one. Too many businesses are complacent about the risk of fraud and think it cannot happen to them. This was the mindset that prevailed at Barings and

led to nine senior executives being barred from the market by the regulatory authority and the Chief Executive, Andrew Tuckey, being disqualified as a director by the DTI.

Fraud risk should be included on the agenda of every corporate strategy planning meeting; it should be raised at main Board level on a frequent and regular basis. Systems and controls should be examined to identify weaknesses which make the company susceptible to the risk of fraud. Employment and recruitment practices should be scrutinised, to ensure that only those new recruits to the business whose references have been taken up and checked thoroughly are employed; that existing staff are surveyed regularly, if unobtrusively, by HR, to monitor their taking of leave, their use of corporate credit cards, their own lifestyles, where this is possible. Many lower paid staff are enjoying a startlingly extravagant private life, with sumptuous houses, cars and mistresses, well known to their colleagues, but often hidden from senior management. Line managers should not be coy about asking the impertinent question, if there is evidence that a staff member is apparently living well above his or her means.

At the same time, clear whistle-blowing policies should be in place in every firm, and employees' attention drawn to them. And they should be workable. Too often, an employee is discouraged from blowing the whistle on corrupt, crooked or dangerous practices taking place in his or her workplace because the very person about whom they wish to complain is the designated recipient of the whistleblowing information.

The Public Interest Disclosure Act 1998 may prove a landmark in the long battle to change attitudes within business. But law alone is not enough. Public Concern At Work's recent paper "Whistleblowing: the New Perspective" by Gordon Borrie & Guy Dehn, points out that someone who informs on corruption in which he or she has participated will receive more protection and help from the authorities than an innocent colleague who reports wrongdoing. Such a situation encourages unscrupulous people to use information for their own advantage and at times of their own choosing.

One solution is to create safe channels of communication to senior management. Such initiatives have developed most successfully in businesses in highly competitive markets where the early reporting of suspected wrongdoing is clearly in an organisation's interest. This involves the provision of alternatives to the reporting of problems via line managers in order to avoid monopolistic control over information flowing up to senior executives. But Borrie and Dehn believe that "the approach many organisations now take to information from workers is similar to the attitude taken toward consumers thirty years ago (that they were troublesome, untrustworthy complainants)".

Companies should, in short –

- Identify the risk areas in their organisation
- Assess scale of risk
- Allocate responsibility for managing risk to a named person or department
- Identify additional controls

- Implement the additional controls
- Monitor implementation of controls
- Evaluate the effectiveness of controls

A policy statement of fraud which most companies could adapt to suit their own particular needs –

- Should apply to everybody in the organisation, including directors and temporary staff
- should demonstrate the organisation's commitment to combating fraud and corruption wherever it is found.
- communicate the organisation's attitude and approach to the threat of fraud.
- The statement should include
    - Allocation of responsibilities for overall fraud management
    - Formal procedures if fraud is discovered
    - Staff training needs
    - Response plans to minimise fall-out.

The statement should be -

- A short, precise document, covering all the points above;
- General review of robustness of existing systems and controls
- Means of regularly testing them
- Identification of assets most at risk

Lastly, the culture of the organisation itself should be assessed to make sure that the right values are emphasised and the lead is given from the top.

The culture of much business world-wide inhibits proper fraud prevention. Of course there can be little uniformity in so large a field and many instances of good and bad practice exist. But a large number of companies may be unconsciously smoothing the way for fraudsters.

The casting and avoiding of blame are common features of business life. Not for nothing has ‘shooting the messenger’ become a standard phrase. It should not be surprising that many employees, often at high levels, prefer to protect themselves, even at the expense of the companies for which they work.

Seeking power through the control of information is also all too common.

Cases have come to light of knowledge of specific frauds being concealed from colleagues. Sharing problems, the better to solve them, is alien to many offices. Here too the ‘blame culture’ exerts its baleful influence. These factors contribute to the failure of so many organisations to aggregate fraud losses. Senior managers define these as an ‘operational loss’, a method that might have been designed to promote crime rather than suppress it. It can amount to systematic concealment from colleagues, shareholders and the authorities.

The public record illustrates the price paid for this kind of business culture. The Bingham Inquiry into the corruption at the Bank of Credit and Commerce

International (BCCI) found that there was an autocratic environment where neither workers nor firms were willing to voice concerns. The European Commission failed to deal with the warnings of one of its own officials who was forced to go public. In these and other cases the results were far worse than if the organisations concerned had faced up to their obligations.

A number of initiatives are attempting to create cultures of transparency with better flows of information and open discussion, aimed at promoting more widespread understanding and better ideas. They go a step beyond Turnbull's valuable but largely systems-oriented approach to risk.

The onus lies with boards to accept that a problem exists, demand information and create policies, structures and procedures. But there is also a need for a different kind of business culture. Staff must feel confident that they will not be penalised for coming forward with their concerns or reporting bad news. Some businesses operate a 'no blame' policy whereby anyone who has made a mistake (as opposed to having deliberately committed a serious offence) can come forward without fear of punishment. The idea is that by cutting out the 'fear factor', reporting of incidents will be improved, thus ensuring the minimum of unforeseen difficulties.

A radical approach is to instil a more highly developed code of moral standards in an organisation by internalising it in individual employees from the lowest to the highest levels, so making everyone responsible for upholding them. An 'internal monitor' setting moral boundaries for acceptable behaviour is the best defence against fraud and failure and ultimately more reliable than rules and structures, essential though these undoubtedly are. This approach is finding favour in the USA and an Association of Ethics Officers has been created. The World Bank inaugurated such a programme in 1998, using a British company to do so. One of the consultants, Tom Oxley, has said that "ethics are more powerful than rules which cannot cover every eventuality, let alone police them."

The views expressed are the speaker's own and should not be assumed to reflect the policy of the Fraud Advisory Panel or its Board.

Fraud Advisory Panel

PO Box 433, Chartered Accountants Hall

Moorgate Place

London EC2P 2BJ

Tel: 020 7920 8721

Website: http://www.fraudadvisorypanel.org