

March 2002

Professor Michael Levi, James Morgan/MorganHarrisBurrows Impact of Crime on Business Study

"Reducing Business Crime - The responsibilities of directors of plcs to consider the possible impact of crime on business, and if necessary to initiate action."

© Crown copyright 2002

Published on behalf of the Department of Trade and Industry (DTI) Office of Science and Technology (Foresight Directorate). Applications to reproduce copyright protected material in this publication should be submitted in writing to: HMSO, Copyright Unit, St Clements House, 2-16 Colegate, Norwich NR3 1BQ. Fax: 01693 72300. e-mail: <mailto:copyright@hms.gov.uk>

The views expressed in this publication should not be taken to represent those of the Department of Trade and Industry

Executive Summary

Levi/MHB Study

Reducing Business Crime - The responsibilities of directors of plcs to consider the possible impact of crime on business, and if necessary to initiate action

Introduction

Criticisms of business for not doing more about crime typically crop up in two key areas:

1. Directors' responsibilities for assessing and reducing the serious risks that crimes can pose for their businesses, e.g. Barings, Maxwell and serious business disruptions caused by frauds, IT failures (from crime or other reasons), and terrorism; and
2. Business responsibilities for the crime risks *to others* that their business processes create or enhance, e.g. the controversies over card & vehicle security and over mobile phones that cannot be de-activated when stolen.

The Turnbull report – which sets out internal control requirements for directors of listed companies – does not deal with the ‘risk to others’ issue, and it was aimed only at plcs, not SMEs. Our aim is to broaden this out with some guidelines for both business sectors and all major aspects of crime.

There are *some legal* obligations on business not to damage society: laws on money laundering, tax evasion, fraud, not intentionally handling stolen property, and health & safety at work/environmental laws. But otherwise, the management of risk to others is left to voluntary choices from a sense of social responsibility, which is often up to the ‘social leadership’ values of particular directors or company traditions, though some former market leaders who have taken the initiative on crime reduction. But it is not ‘just a social issue’: reputational damage is the other face of valuable corporate ‘goodwill’ and, as the case of accountants Arthur Andersen has dramatically shown, such value can vanish very rapidly if firms lose the confidence of their customers, partners and/or shareholders. Key to business prosperity and even survival is the physical integrity of the firm’s products (or apparent products, since pharmaceuticals and vehicle parts that harm users are sometimes counterfeits) and the public’s beliefs in the financial integrity of its products. There is appropriate flexibility about which risks are material: since September 11, many large businesses have worked hard on the physical security of senior staff & buildings, even seeing unauthorised access without loss as a symptom of the possibility of terrorist attacks succeeding. What is often below the radar are high volume, low individual impact crimes: companies sometimes fail to aggregate these and – as many corporate frauds like Barings and the US branch of Allied Irish Bank show - they can creep into ‘materiality’ without anyone noticing. Directors sometimes take their eyes off the ball with subsidiaries and business units that may manipulate performance, and it is vital to install systems that pick up discrepancies and abnormal patterns of trading that may conceal trading losses, thefts or money-laundering.

Not all crimes are serious threats to business, but without taking the crime issue seriously, directors have no obvious way of appreciating their current and potential impact. There are six simple steps to identify and deal with most crime risks *against* the firm, which apply both to plcs and SMEs and that we would regard as components of ‘corporate life skills’:

1. *Establish the nature of the business and the financial & reputational risks that crimes might bring*

- This is not just an issue for plcs, though plcs may be more likely to suffer from failing to avoid laundering money for corrupt politicians, drugs traffickers and terrorists, from serious employee or management fraud, or from product contamination. But having staff who cheat customers or demand bribes from suppliers, or high profile crime events that depict the business in an uncaring light or as ‘promoting crime’, can destroy the brand value or the long-term trust in the managers or even in the trade. Major credit frauds by purchasers can dramatically harm SMEs, and it is vital for them to appreciate that relatively small crime losses compared with those in plcs can be catastrophic. The proper way of looking at harm is to calculate what we term the ‘recuperation factor’: how much business would have to be done to recover the losses from crime. The smaller the profit margins and the lower the capital base of the firm, the greater the recuperation factor.

2. *Look at actual crime experiences within the firm*

- Between the vulnerability and the experience is often a gap, so check out systematically how many times and under what circumstances crimes have occurred

3. *Look at the experience of comparable organisations and benchmark*

- Crime vulnerability should not be a competitive issue. Larger firms may have opportunities for security professionals to share experiences and build up a quality circle to reduce risks

collectively, but even smaller firms can co-operate to check if others are preventing crime risks that they are not.

4. *Define information requirements and establish routines to:*

- Encourage the reporting of all crimes and threats, collate this data, and analyse, present, report and act on it.

5. *Establish cost-effective programmes for review, control and prevention*

- Here, we emphasise that stopping frauds from continuing is an important form of prevention, and that intensive reviews of bad debt can pick up a lot of fraud vulnerabilities; and

6. *Have a post-event strategy and plan.*

- Firms that really get punished are those who do not plan for business interruption or reputational risk and react with panic or poor judgement if it happens.

'Government', 'business', and 'police' do not currently share a common perspective on crime issues, nor do all their component parts have a common outlook. We suggest separate action points for each sector, to increase responsibility for and ownership of the crime problems. Of course it is important for all three to work together, but this should not be taken as an opportunity for individual problem evasion. In stating this, it is important to be clear and not to engage in wishful thinking. The market does not provide an automatic short-term mechanism for crime reduction either against business or by business against the community. Experience suggests that except for some adjustments taken to set a corporate tone, the biggest impacts on those crimes that are *facilitated* by business lie in (a) making and enforcing regulations or criminal laws imposing a legal obligation on business, or (b) generating a reputational benefit or damage that affects the bottom line in sales or in the investment community can be addressed only by legal requirements or by negative/positive publicity. The Home Office publication of a 'car stealability index' is one example of (eventual) action without legislation; but legislation on money laundering and transnational bribery was used as a springboard for consultative arrangements to reduce those crimes. In payment card fraud, key parts of the industry developed co-operative modes of information sharing and intelligence-led private policing to reduce crime well below what it would otherwise have been, but few public resources have been available for backing up these measures in the criminal justice sphere. The key ways forward for crimes against business are:

For Business:

1. *Publicity. Make advance plans so that when a major crime causes a substantial and/or sensitive business failure, ensure there is well informed comment on the general nature of the business risk [avoiding the shrinking violet of "it's all sub judice"]*
2. *Wind crime risk management issues into all the business' operating, financial and HR systems and approaches, including those such as Investors in People etc.*
3. *Train mainstream staff in businesses – not just the accountants- in crime awareness*
4. *Identify risks better and think how much less business you would need to do if you could cut crime costs without sacrificing too much sales: sales that are not paid for are unproductive!*
5. *Share crime data better to develop a better benchmarking of crime (including fraud) risks, and ratchet up the skills levels of internal audit, security and credit control departments including getting them to talk to each other more.*

For Government and Police

6. *Ensure that the subject of business crimes has a real home in the right Department. The Home Office has not actively promoted evidence-led policy on business crime, but has played a key role in 'encouraging' some business sectors to design in prevention by publishing risk information. Only the Home Office can influence policing priorities. But the DTI can play an important role via winding director disqualification, company regulation and company law reform into a coherent inter-departmental business crime reduction strategy, while the FSA has a key role in financial crime reduction for regulated firms*
7. *Appreciate that if the police and police authorities do not know about large chunks of crime - those committed against business – they cannot readily fulfil their responsibilities for crime audits and reduction strategies for their areas, nor is it obvious how they can build a proper criminal intelligence model*
8. *Keep up the pressure on the CBI, FSA, the fiduciary professions, etc. over the issues as well as acting as a conduit for their views*
9. *Run PR campaigns and prizes for innovative actions taken by businesses – and perhaps the wooden spoon for most foolish/crass corporate victim, unless that would deter reporting of fraud to the authorities*
10. *Establish a real programme of education and training for the police, alongside people from business, combined with a sense that this work is valued and is a core part of the policing function*
11. *Establish integrated private sector- police jointly funded initiatives aimed at crime reduction as well as crime investigation: it is the latter that makes most sense to business*
12. *Ensure that the police are aware of the costs that crimes against business impose not just on profits but on amenities for the public – many poor areas are blighted because businesses find it too risky to operate there.*

Civil Society

13. *Integrate crime risk management into the business school curriculum, and draw on case studies not just like those provided by Enron, Arthur Andersen and Allied Irish Bank but also by smaller but material-to-SME business cases. The neglect of fraud and corruption issues by many business schools raises serious issues about their preparation of MBAs, not so much on business ethics as a philosophical subject (which is better catered for) but on financial and reputational risk management*
14. *Encourage shareholder, especially institutional shareholder, and lender pressure in relation to crime risks (a) against the company directly and (b) that can generate reputational risks for the business though the direct victims are outside. Plc directors have to rehearse responses to questions that relevant shareholders or lenders may ask them about. If their crime reduction, crisis response and disaster recovery processes are things they will be questioned about, they have greater incentive to find out what might cause them serious risks.*

In short, in our view there is a need for a rigorous strategy and set of action plans with external performance evaluation, rather than relying on one more document to "turn the corner".

Reducing Business Crime - The responsibilities of directors of plcs to consider the possible impact of crime on business, and if necessary to initiate action

Introduction

Crime can affect business in many ways: it can generate direct financial losses, and can generate reputational damage which can destroy shareholder and owner-manager value, and divert senior executives from business into crisis management. Despite this, there is no requirement for business to guard against crime in general terms. The closest we have come to guidance on this issue is the Turnbull ^{*1} report of 1999, which stated that crime could be included as a specific risk that directors of public limited companies need to address and report on to their shareholders. The Crime Prevention Panel subsequently proposed that this was a positive way that crime could be incorporated into the mainstream of business decision-making.

Professor Michael Levi of Cardiff University, and James Morgan & John Burrows of MHB were commissioned by the Business and Crime Task Force to identify, in the light of Turnbull, the full range of ways in which crime can be a risk to businesses. This report aims – to the extent possible in the very modest time available to us – to address the specific terms of reference provided by the Task Force:

1. *Set out how crime can damage business;*
2. *Review how business might assess the cost of crime to it;*
3. *Identify steps that might be taken to address these threats;*
4. *Present all the information as guidance points for senior executives; and*
5. *Make recommendations on the best way to get the information over to businesses at all levels.*

Turnbull offered guidance to directors of Plcs focussed on their responsibility for ensuring that the company assesses and manages its business to address significant risks: those identified by senior management as being potentially damaging to the achievement of the company's objectives. *It was not aimed at crime reduction as such, but only at those crimes which truly stop management getting their core job done, and might count as sudden unwelcome surprises.* This encompasses a wide range of issues, internal and external, from (a) any actions that generate a negative perception of the business through (b) previous criminal/disreputable actions (known or unknown) of senior executives while with other firms, to (c) crime as commonly understood. Furthermore, though not mentioned in the report itself, the 'due diligence' enquiries that have become a generally accepted feature of Mergers & Acquisitions activities may require acquirers and target companies to have in place reasonable risk identification and management processes. So – whether or not they are listed on any Stock Exchange - it may be in the best interests of domestic or international companies to take some note of the Turnbull and other 'corporate governance' principles. In this sense, the internationalisation of business is driving expectations up.

*1 Internal Control: Guidance for Directors on the Combined Code, ICAEW.

'A company's system of internal control has a key role in the management of risks that are significant to the fulfilment of its business objectives'.

The guidance indicates the company's internal control system should:

- be embedded within its operations and not be treated as a separate exercise;
 - be able to respond to changing risks within and outside the company; and
 - enable each company to apply it in an appropriate manner related to its key risks.
-

The origins of the Turnbull Report lay in the failure and/or perceived failure of successive gestures towards better corporate governance during the 1980s and 1990s. Maxwell, Polly Peck and a host of other major corporate failures had highlighted the relative inattention at Board level to the possible causes of catastrophic fraud - whether in one major hit or, as in these cases, over a period of time. It is beyond our brief to review whether Turnbull was either a necessary or a sufficient response to those scandals: as has been alleged in relation to the collapse of Enron, charismatic and bullying senior executives who *de facto* pick their non-executives may be able to by-pass formalistic controls in almost any system.*2 However, the attempt was made clearly to fix responsibility on *those items of crime that have a material impact on the profitability or viability of the plc business: the risk of fraud was the only crime specified in the report, but safeguarding of assets from inappropriate use or loss was included.*

Our gap analysis leads us immediately to note three major areas with which government and the public may be concerned but which 'fall below the Turnbull radar'. These are:

1. The non-application – except via some questionable trickle-down effect - to those businesses that are not plcs. In particular, Turnbull is unlikely to have much effect on the SME sector, and it is precisely these businesses which have been a constant source of concern in the business crime prevention literature;*3
2. The apparent lack of need (at least by Board members) to deal with crimes below 'corporate materiality' levels,*4 even though such crimes can be of very significant 'public concern'. In our view, materiality has to be separated into (a) the 'objective' cumulative total and (b) the reputational effects which are a result of rumour/media-generated market suspicions, insider leaks and/or criminal justice actions;*5 and
3. the apparent irrelevance of 'crime externalities' generated – intentionally, recklessly or inadvertently *6– by the company's core or marginal business. For example, mobile phone robberies from individuals *7; or the ease with which offenders can dispose of crime proceeds, etc.

We shall have more to say about these significant omissions later, but we stress that whatever readers' personal feelings may be about the moral claims of corporate responsibility, there is no legal obligation on any company to do more about any of the three items above than they are minded to do in furthering shareholder or private interests: except when specifically mandated by law, as is the case with the requirement of regulated businesses to have adequate anti-money-laundering systems in place and to report to the National Criminal Intelligence Service those transactions that they suspect of being aimed at financing terrorism or laundering the proceeds of any serious crime. Arguably, it is not within the ambit of auditors to comment on any of these voluntary issues either. In reality, there is much scope for ambiguity.

Such ambiguities are reflected in longer-term corporate relationships with the community and with government (sometimes via the media) – encouraged by Cadbury and Turnbull. They are part of a wider Western 'social responsibility' trend to be found also in the US. Similar ambiguity is also evident in the possibility that any routine 'crime' (which may manifest itself as an ordinary business loss) may escalate into a 'material business risk', whether or not it involves any active complicity of management. One problem here is that the definition of the loss as a crime is often not straightforward, especially with credit frauds: and so the discernment of a pattern, likewise, is problematic. Our interviews reveal that, especially since September 11 2001 (hereafter described colloquially as '9/11'), and most particularly in the case of the US-headquartered and multinational corporations, major reviews of security risks have been undertaken in which even minor thefts by infiltrators or contract staff are being treated as material, since they indicate control weaknesses that could have led to terrorist attacks. In some cases, Boards have spent substantial amounts of money in external testing of

security arrangements. In our view, this change in the materiality status of 'minor intrusions' represents a reasonable management response to a changed risk climate. [*8](#)

***2** Though it remains obscure to what extent non-executives did address their minds to the risk of management fraud, and what skills would have been required to enable them to address those risks adequately

***3** For a recent effort to guide SMEs, see Fighting Fraud - a Guide for SMEs, Fraud Advisory Panel, 2002.

***4** This can descend into tautology because one may know that an issue is material only after it has generated serious problems. There is either over-prediction or under-prediction of materiality of risks.

***5** One of the grievances expressed strongly by some corporate directors and security managers was that 'even if we spend time and effort on pursuing a prosecution, nothing significant happens to the criminals': in their view, white-collar crimes against business are treated so leniently that there is little deterrent effect from the criminal justice process. This also can affect the willingness to report crimes.

***6** The application of any of these epithets is a matter of judgement on which reasonable people may disagree.

***7** The £4.2 million of mobile phones taken from a London warehouse in February 2002 might, however, count as material, even though they were subsequently recovered (for the latter would not have been a probable outcome of the business plan).

***8** It can always be argued that the terrorist risk was there before, but there is a limit to how much management can and should spend on such risks, and the assessment of probability of occurrence of rare events is far from objective science.

In a 1999 report for the ICAEW, Implementing Turnbull, the authors cite a Deloitte & Touche survey of significant risks perceived by management. The only one directly related to crime is "poor reputation" (or "brand management"). However, crime can affect other identified high risk factors such as employee morale and failure to manage major projects (especially those overseas). But previous work in this area does not make it at all clear how businesses can best be persuaded to manage systemic and individual corporate risk better.

In our view, the actual effects, or possible risk, of reputational damage depend upon:

1. the pure economic responses of customers and suppliers;
2. the effects on potential M&A participants (national and international) of scandal or of "due diligence" enquiries indicating potential serious underlying business risks;
3. regulatory action (if subject to regulatory discipline, including stock exchange listing and audit);
4. shareholder reactions; and
5. HR implications for staff recruitment and retention.

All of these vary by industry and also by the initial reputation of the firm and the motives of key stakeholders. Reputational problems facing (mis)sellers of long-term financial products such as pensions and/or international retail/wholesale banks (e.g. Allied Irish Bank through its separately managed American subsidiary Allfirst) are plainly different from those facing – say - tobacco industry firms which are already in an officially stigmatised industry. [*9](#) The former also have a risk-based regulator whose task - with limited resources - it is to ensure that the businesses in this area are run in such a way that the public are safeguarded from loss and risk of loss. If internal compliance systems are deemed to have failed, firms as well as individuals can be de-authorised under the Financial Services Authority rules, far more readily than in the non-regulated sector, where except in very rare circumstances, action against directors will only be taken after liquidation. [*10](#) Put differently, the 'materiality level' is quite low for fraud against the public and for infringements of business processes

that could lead customers to lose out. For this reason it is necessary to recognise that different considerations will, in practice, apply, on the one hand to regulated financial services industries, and, on the other hand, to the non-regulated sector: [*11](#) while acknowledging that there is much intra-sectoral variation.

Trust (and a reliable legal system where this is absent) is now understood to be a central theme and precondition underlying the success of capitalist economies. (Conversely, the absence of trust is a major feature inhibiting the development of *criminal* organisations.) The importance of establishing trust may be seen in a range of contemporary issues – GM foodstuffs, MMR vaccines, and post-mis-selling financial services – in which the credibility of claims made by authority figures is doubted by important sectors of the public. The globalisation of business generates greater risks that some of these groups may have legal standing in some jurisdictions to sue companies for foreseeable risks that led to them suffering harm. These lie outside our remit, but we simply point to the paradoxical ‘scandal fatigue’ effect: namely that low public expectations of a business or businesses may reduce the impact of negative publicity on corporate sales. In contrast businesses can face serious risks to their future from crime losses that affect the bottom line, irrespective of any reputational damage. Some insurers may require companies to address crime risks as a condition of insurance, while others may respond (as in IT) by excluding cover, creating further pressure to manage those risks to avoid material loss.

***9** Though there is an absence of firm evidence of the impact of scandal on product demand (see M. Levi and A. Pithouse, forthcoming, *White-Collar Crime and its Victims*, Clarendon Press).

***10** In practice, large firms' size may protect them from de-authorisation, but individuals are more vulnerable. Companies may be closed down under the Companies Acts 'in the public interest', but normally if they are posing a risk to private individuals rather than to businesses, e.g. wine and spirits companies taking in effect 'investment funds' on the basis of unrealistic claims about future values. The latter are not covered by the Financial Services legislation since they are not deemed to be investments within the Act.

***11** Accepting that all plcs are regulated by the DTI (in relation to the Companies Acts) and by stock exchange listing requirements, sometimes in several countries.

How can crime damage business?

This section sets out some of the main areas of crime risk, and we suggest an approach that businesses can take to develop their own risk profiles. One of the most important tasks of the Board and senior management in any business is to set clear guidelines for the operations of the business and its future development. In setting these guidelines they will require clear consideration of the main sources of risk that could materially disrupt either current operations or the future development of the business.

For almost every kind of business, crime is a potential source of risk that could have a materially disruptive effect. Crime can have its effect on the business in a number of ways, which range from:

- "Catastrophic" single major hits. For example, arson or terrorist attacks causing the destruction or serious interruption of major business assets, or a major fraud like the transfer of many millions by a member of staff or Director. The impact of such catastrophic hits depends on the capital base of the business;
- Criminal acts where individual occurrences have comparatively little impact on profitability, but where the cumulative effect of repeated occurrences can lead to

- business failure; and
- Crime which may not damage the business directly but which can have a significant effect on the reputation of the business.

Our interviews with executives, coupled with the evidence from surveys, suggest that businesses' main concerns are in the area of catastrophic failure caused by fraud and faulty business process. Some British companies were already taking significant steps to deal with business interruption in the aftermath of terrorist attacks on Bishopsgate, Canary Wharf and Manchester, assisted by both special and general [*12](#) warnings from police/Security Services sources. Undoubtedly, and especially in the case of US-headquartered corporations, these security precautions attained higher profile and resourcing post-'9/11'. [*13](#) Such focussed reviews of security risks, covering both staff and business processes, would probably have occurred irrespective of any corporate governance recommendations. To develop further professionalism in the security management aspects of the banking sector, some major international banks have developed an informal peer group within which to discuss best practice and to ratchet up standards. There are several other such security groupings, both within industries (such as petroleum producers & retailers) and across sectors, in professional associations.

In the case of fraud, the focus on key 'bad hat personalities' such as Nicholas Leeson and Robert Maxwell - earlier analogues, it is alleged, of John Rusnak of Allied Irish Bank and Messrs Skilling & Lay of Enron - around whom crime was concentrated promotes the view that these were one-shot catastrophes, whereas in reality they were cumulative, long-term catastrophes, even though they were the products of the dangerously fertile minds of key individuals. The Sherlock Holmes question of 'why didn't the watchdogs bark' (not just in the night but also in the day) remains important, but the Allied Irish Bank/Allfirst case of 2002 seems to illustrate the fact that dangerous acts can be committed by apparently ordinary individuals who would have passed ordinary vetting criteria. [*14](#) This focuses our minds on the infrastructure and control weaknesses which enable crimes to take place and on the bonus and status pressures that - given the unregulated opportunity - make violation more probable.

The dynamics of such frauds often involve a zone of 'free experimentation' in which - to the surprise of offenders - controls are not exercised, enabling risk-favouring individuals to progress further and test the limits of the system. Sometimes, the offenders stop and are never discovered; at other times, as alleged in Allied Irish Bank, the behaviour can carry on for years. Again, it is difficult to point to a specific moment at which such frauds become material (except in hindsight): but all control weaknesses that do not have monitoring and alarm mechanisms are Turnbull-material for Boards, if and when they find out about them. Such dramatic events do concentrate executives' minds on reviewing risks and controls, and benchmarking is also likely to occur at such times. In this sense, the business sector learns from public revelations of victimisation experiences and, largely unprompted by Turnbull, takes what it hopes will be remedial measures. Equally, in some security fora in which there is high interpersonal trust, businesses also learn from private information sharing about unpublicised cases. [*15](#)

[*12](#) Though some commented that the warnings were overly general at times, making risk judgements very difficult. On the other hand, this may reflect the reality of intelligence source uncertainties.

[*13](#) One major international bank spent over \$55 million more annually on more professional guarding and a one-off further \$211 million on technical physical security measures after a risk-based review.

[*14](#) Ironically, Leeson had been deemed not fit and proper by the predecessor of the Financial Services Authority in the UK, following which he was transferred to a location in which less control was exercised over his activities, illustrating the theme that where businesses are global, disposing of problems in one jurisdiction can lead simply to displacement or worse.

[*15](#) For example this is done through the Risk and Security Management Forum (RSMF), which naturally operates under 'Chatham House rules'.

It is clearly not possible to document all forms of 'material' risk, but some examples might be:

- False Accounting

One of the main ways in which fraud affects businesses is through "false accounting". Often this will not mean that there has been physical theft from the business but that executives will falsely report results in order to conceal their own poor performance – and perhaps to protect bonus payments based on reported company performance. They may not intend to be around long enough to suffer personally the consequences for the company and to that extent, this represents a weakness in the processes for ensuring long-term shareholder value maximisation. This is relatively common in business cultures where Chief Executives, whether of the top company or of subsidiaries, are given "demanding targets with little interference from above or detailed business controls". *16 An example is provided by a UK university that acquired – at a cost of one pound - a major research institute that had previously been part of a government department. Work in progress was mis-stated by reporting project over-runs and speculative work as profit earning, even though it was not possible to recover the costs from the institute's (mainly public sector) customers. The final loss to the university ran into tens of millions of pounds.

- Deception

The most straightforward form of fraud involves deception that is used to conceal theft and its effects. There are many examples, frequently reported in local newspapers, since unless the sums are huge, this form of crime is so common it is not thought newsworthy for the national papers. A typical example is purchase fraud where payments are made to a phantom supplier. Cheques are issued and paid into an account controlled, perhaps through an alias, by the fraudster, who might typically be in the accounts or purchasing departments of the company. A variation on this approach is where a real supplier is prevailed upon to over-invoice. The payment is authorised by the fraudster and the surplus is divided with the supplier. Of course there are great opportunities for corruption and blackmail in this approach.

- Long firm fraud

Intentional credit frauds against companies have many and varied effects, some having the same nature as routine credit losses (whether defined as such or defined as fraud) and others being severe, especially to SMEs. In one case, having been lured with the prospect of a big bogus order, a supplier lost almost his entire annual output of Christmas trees. There are also secondary effects that may produce temporary benefits for consumers, as unpaid-for goods undercut legitimate stores in an area and drive them out of business.

- Kidnap/ransom

Has been relatively uncommon, but not unknown in the UK. *17 But it is a real risk that must be considered by businesses which have operations in countries where violent crime is more common than in the UK. Of course, where the directors and senior management of a company, based in the UK, have relatively little experience of operations outside Britain they will need help and support in assessing these risks. Even companies with a great deal of relevant experience are not immune from this kind of crime. For example, the Chief Executive of a substantial South American subsidiary of a major UK company with world-wide operations was kidnapped and

held by guerrillas for almost a year. One of his trusted bodyguards was complicit in the kidnap. Although the company has never confirmed the story, it is believed that a substantial ransom was paid.

- Arson

Can be a risk, not just as a consequence of vandalism, but also to cover up traces of theft or other crime. It may also be a revenge action by a disgruntled employee or ex-employee. Insurance companies will also point out that arson frequently occurs when a business is failing. In one instance a City of London investment institution had funded the take-over of a boat building company, taking note of the valuation of the assets. On the morning of the day when the new owner arrived to start work in the business he found that a major fire had destroyed all the work in progress, and the company records during the previous night.

- Theft

Is a relatively common experience for businesses of all sizes, and can be particularly debilitating for SMEs. The Small Business and Crime Initiative (supported by NatWest), which promoted measures to protect small businesses from crime, showed that small businesses were over five times more likely to be victims of burglary than domestic properties (see Wood et al, 1997 and Tilley and Hopkins, 1998). *18 In one case a fashion designer's premises were broken into and the whole collection stolen just before a major fashion event. The result was the complete loss of a year's work. And, of course theft in the retail environment is a routine concern for retailers. In fact, crime in the retail sector is the only form of business crime for which there is any routinely available information (see, for instance the annual British Retail Consortium-funded crime surveys). *19

- Product piracy

One of the most contentious areas of harm, the counterfeiting of legitimate products with no safety implications, raises difficult economic questions. Not all goods counterfeited would have been purchased, since many purchasers could not or would not afford them. However, there have been large genuine opportunity costs arising, for example, from businesses that buy counterfeit software substantially under value. Unfortunately for the industry, digital products are not degraded by copying, so the purchaser does not get an inferior product.

- Product counterfeiting

Although in some areas of business it can be argued that counterfeited products are not harming the general public, this is not the case where counterfeit, or substitute, products using poor quality materials are used in safety critical applications such as replacement aircraft parts, or, a more common experience, brakes and steering components for cars and commercial vehicles. Frequently low quality replacements are fitted during maintenance and owners are charged the full price applicable to genuine parts. In one instance, a company was supplying to customers in a developing country replacement wearing components for earth-moving equipment made of inferior quality, cheaper steel rather than of the higher quality steel originally specified by the equipment manufacturers: but it continued to charge 'top whack' prices. Such behaviour is material to the company if it is discovered, or likely to be discovered: but executive interest may depend on whether it is done with the active or

passive/deniable connivance of the Board, or whether it is a corrupt racket by junior staff.

- Hacking and denial of service attacks

Are subjects of increasing concern to business: a fact confirmed by all commercial crime surveys, whether or not justified by real increases in incidence and prevalence. In most cases in which hacking is (a) detected and (b) something is done about it, this imposes some costs in terms of updating controls. In some cases the result can simply be one of nuisance. But, at the other extreme it might be loss of very valuable intellectual property in the form of designs or research results. All companies will be concerned about the possibility of hackers gaining access to computer files that give the possibility of financial loss. For example by the hackers inserting themselves as creditors, or even employees of the business or eliminating themselves as debtors. Financial institutions will be particularly concerned that hackers might use the access they are able to gain to divert cash away from the business. In one instance a disgruntled sub-contractor, who had the necessary computer authorisation, accessed the computer systems of a public utility remotely. His declared intention was to complain about controls he believed were inadequate. The result of this intervention was to disable a "business critical" system for twenty four hours with a consequent loss of interest, because invoices could not be sent out, amounting to several millions of pounds. This case, too, illustrated the difficulties of pursuing action under criminal law when the damage was suffered by the organisation whose computer was in one UK county but the criminal himself, his actions, and consequently the investigating police force and CPS were in another part of the country. In other cases, the 'spoofing' of corporate web-sites such as AOL can generate the divulging of credit card and other personal information enabling large numbers of frauds to take place at the expense of genuine card-holders, damaging the reputation of the spoofed company without necessarily losing them money directly from the scam.

- Corrupt inducements (national/transnational; and against the company/for the company)

A long-term contract for supply of waste products at disadvantageous terms between the company and the finance director's brother in law's company operating through nominees brought the company's profits down to negligible levels. On the other hand, the alleged corruption of 'politically exposed persons' (high-status public officials) by British companies may have brought orders to them, though others have lost orders to corrupt or more corrupt competitors from other countries. However, the OECD Transnational Bribery Convention 1997, brought into effect in England and Wales by the [Anti-Terrorism, Crime and Security Act 2001](#) and now in force, has ratcheted up the potential costs of engaging in transnational corruption. There are also implications for the reputational risk [*20](#) and money-laundering legal liabilities of financial institutions and of law firms processing these bribery transactions.

- Money Laundering

Irrespective of whether or not a bank is prosecuted or good clients desert the institution, revelations of money laundering are extremely expensive in management time, and can - along with frauds - lead to exclusion from syndicated loans and other trust facilities. Where a corporation is headquartered or has a significant subsidiary in a jurisdiction which is 'blacklisted' by the Financial Action Task Force, this can have a material effect on profitability. The Bank of New York's poor internal controls over dealings through its London office and disreputable corresponding banking clients led

to widespread humiliation and management costs, even though in the aftermath of the clean-up, profits and share prices rose. [*21](#)

*16 John Smart of Ernst & Young - private communication

*17 For a thoughtful review of this subject, see R. Briggs (2001) *The Kidnapping Business*, London: the Foreign Policy Centre. In our view, it may become more common as target-hardening reduces crime opportunities in other spheres. However, police successes may have deterred some from considering it as an easy option.

*18 See Wood, J., Wheelwright, G and Burrows, J (1997) *Crime against small business: facing the challenge*. Crime Concern; Tilley, N and Hopkins M (1998) *Business as usual: an evaluation of the Small Business and Crime Initiative*. Police Research Series Paper 95. London: Home Office

*19 BRC survey. Note that for the retail sector, fraud (other than management fraud) risks are a minor proportion of the total crime problem.

*20 It could be argued that there is reputational risk if there is publicity independent of prosecution. But publicity tends to be greater and the media less libel-shy if there has been a prosecution or some regulatory action (see further M. Levi and A. Pithouse, *White-Collar Crime and its Victims*, forthcoming).

*21 Part of the reason for the Bank of New York's survival/prosperity despite the public shaming was that it had some major comparative advantages in global custody services which were in short supply and which were not threatened by the revelations in which clients lost no money.

Creating a business risk profile

Every business has its own risk profile and "Business crime" needs to be broken down into categories appropriate to the business. A matrix categorisation may be helpful:

- Type of business ownership
- Business sectors and sub-sectors
- Classes of crime

These broad headings can then be broken down into:

Type of business ownership

- Owner managed
- SMEs
- Shareholder owned larger businesses
- International operations (foreign law e.g. product safety or transnational/local corruption legislation/expectations may be an issue)

Business sectors and sub-sectors

- Business sectors and sub-sectors
- Business processes

All sectors, and especially sub-sectors, have different risks and are more vulnerable to different forms of crime.

The categories may be more appropriate to SMEs than to large companies, but one of the most

sophisticated studies - the Scottish Business Crime Survey *22 - showed that the top five sectors for reported crime were:

Restaurants/takeaways	983 incidents per 100 premises p.a.
Public transport	962
Motor/fuel retailing	690
Post/telecommunications	642
Pubs and clubs	613
General retail	569

Access to reliable crime statistics is limited to the few surveys that have focussed specifically on business crime. Police forces' counts of recorded crime do not distinguish the characteristics of crime victims, making it impossible to distinguish how many related to businesses, let alone any more refined sub-sets. The British Crime Survey, which is increasingly used by the Home Office as the main indicator of the extent of crime in the UK, is based entirely on surveys of householders and deals with personal and household crime only. Moreover it is important to note that such official statistics as there are concentrate on the 'incidence' of crime. That is the number of incidents of crime reported to the police, or experienced by victims, and not the cost of the crime to the victim. 'Incidence' is not the same as economic impact. The cost of crime is frequently not examined in any depth, even by victimised businesses, and is not reflected in any official statistics about crime.

Classes of crime

- The business as a victim (e.g. theft)
- Individuals as victims in the context of business operations domestic and overseas (e.g. robbery, kidnap)
- Products and processes generating opportunities for crime (e.g. cybercrime)
- The business and individual employees treated as offenders (e.g. criminal negligence, equalities issues)

*22 Burrows, J., Hopkins, I., Bamfield, J., Hopkins, M. and Ingram, D. (1999) *Crime against Business in Scotland*, Edinburgh: The Scottish Executive Central Research Unit.

Assessing the potential cost of crime to business and steps to address the threats

Some crimes have a catastrophic impact on business: for example, 9/11; Barings; or Maxwell. In the case of management fraud, one of the classic warning signs is a single bully with concentrated powers at the head of the organisation. But, as Sir John Banham has pointed out, poor corporate governance is not necessarily reflected in low returns to shareholders,*23 nor is good governance, measured by separation of executive and chairman functions, reflected automatically in high shareholder value. However, businesses will have little experience of the impact of this kind of crime until the problem actually hits them. Nor are there any valid statistics about the incidence of this kind of problem in business in general to give any guidance, or comfort. But there is a need to review and assess the risks.

In many fields major disasters occur through a combination of circumstances. For example an event occurs and planned counter-measures and recovery processes don't work, often because they're out of order. But sometimes because the need for defensive measures is completely ignored: the standard response to the question "where were the auditors?" when a catastrophic failure has occurred is that management has the primary responsibility for safeguarding the shareholders' assets. The common scenario in many major crimes that cause business failures is that a combination of risks – anticipated or unanticipated individually but not anticipated collectively - have gone wrong. This was amply illustrated by the Barings case, where: a) Leeson acted illegally to try to cover up trading losses; b) local management failed to do its job; c) senior management in the head office failed to do their job; d) business controls didn't work; e) neither internal nor external audit provided any protection. There are, however, sometimes instances – as post 9/11 – when out of comity or from a desire to avoid systemic risk, other businesses help out those who have failed to ensure business continuity in the event of disaster (e.g. Bank of New York and, in a different context and with both governmental and private sector assistance, Long-Term Capital Management).

Some kinds of crime will have less impact as individual occurrences, but will have a more cumulative effect if the crime continues un-addressed. So there is a need to assess the potential impact of this kind of crime on the business. In this area there are a range of documents – from government departments, trade bodies like the CBI and British Retail Consortium, from professional bodies such as the ICAEW, from quasi-governmental organisations like Crime Concern, Victim Support and the HSE, and from firms of forensic accountants – that outline the basic steps businesses need to take. In our view, neither consumer pressure nor the market left to itself will always provide a solution to these crime and security problems, and we have to gear ourselves to confronting them continuously or periodically rather than searching for a 'silver bullet' that will eliminate risks once and for all.

It is not enough for a business just to identify the possible risks that it faces. It also needs to assess the possible impact of these risks, the probability of these risks arising (a far from easy exercise) and finally it needs to consider the appropriate response. This section sets out six steps a business can take to achieve this. There are various permutations to this advice but abstracting the highest common factors, most advocate six simple steps that we would like to term 'corporate life skills' and that apply across the board to all firms, whether plcs or SMEs.

*23 The Sunday Times, 10 February, 2002. The fallacy in this position is that it ignores whether catastrophe fraud is made more or less likely by failures to separate functions and ensure independence. However, we would accept that formal independence is not a guarantee against 'capture' by dangerous charismatics.

Six Simple Steps

1. *Establish the nature of the business*

- Type of business ownership
- Business sector and sub-sector
- Classes of crime

2. *Look at actual experience*

- How complete is the information available? (are some crimes not reported up the hierarchy? Not noticed? Not detected?)
- What risk analysis is undertaken at lower levels in the business?
- What is the actual incidence of different types of crime and their economic impact on

the business?

- What is done to prevent the crimes or recover losses?

3. *Look at the experience of comparable organisations*

- Establish the general level of experience, by reference to industry data, where available, having regard to type of business, industry sector/ sub-sector.
- Establish expected performance, set targets.

4. *Define information requirements and establish routines to:*

- Encourage the reporting of all crimes and threats, collate this data, and analyse, present, report and act on it.

5. *Establish cost-effective programmes for review, controls and prevention*

- As with any business challenge, imagination and ingenuity is required to reduce known losses or anticipated risks. Even when responding to simple theft, there will be many alternatives to simple 'bolts and bars' solutions. There will often be a need for experimentation and evaluation of different options.

6. *Have a post-event strategy and plan.*

- Contingency plans need to be put in place for taking action when significant crimes affect the business, or when investigation is needed to follow up suspicions that such crime may have happened. Moreover, 'when the dust settles' it also crucial to scrutinise, in detail, what went wrong and how to avoid repetition.

Guidance for Board Members

At a minimum, Board members need to ask these four questions:

1. *Has the business reviewed the risk to itself from crime?*

- What resulted from the review? What action has been taken?

2. *What are the major threats?*

- *And what action has been taken/is planned to prevent/address the threat?*

For example

Threat

False accounting: subsidiary reporting excessively optimistic results

Counter-measures

Adequate management information; control over cash; review of management reports; internal audit

Shop theft	Control over cash on a daily basis; CCTV; staff training
Purchase Fraud	Management controls; standard costing; internal audit
Loss of intellectual property	"Need to know" security policies; HR policies; IT security systems
Burglary, Theft	CCTV; Alarm systems; perimeter security
Money Laundering	Normal well understood ones plus correspondent banking relationships are a key reputational/legal risk

What is the actual experience of the organisation?

3. *What is the post-event strategy and plan*

Recommendations for Change

There is no shortage of guidance material. There are plenty of reports, documents, videos etc. by bodies such as the CBI, British Chambers of Commerce, forensic accountants, Fraud Advisory Panel, Audit Commission, Home Office, National Audit Office, and even some academic studies of crime at work. The problem is, rather, getting people to take notice of it. Business crime and business related crime is almost an unmentionable: a kind of corporate halitosis. As one of us (ML) wrote beginning an article in *The Company Lawyer* 20 years ago:

Commercial fraud is rather like venereal disease. Neither the victim nor the perpetrator wants to talk about it. Those who are neither don't want to talk about it in case others think they have it. And not talking about it does nothing to stop it spreading.

The subject of crime in business has moved on, and while it does feature in business journalism, this is generally in scandal terms (mostly when there have been 'material' effects on business, which effects are increased by the publicity) rather than on the everyday risk that businesses face. Rather, the pretence is that when major crime is evident, it is an aberration caused by the combination of truly evil individuals and truly stupid Boards. Business ethics has become a growth industry – though with what effects on business practice remains a matter for speculation. However, we found almost no evidence that the subject of crime is addressed in business schools as a business risk or in the case studies on which the business school teaching is based. Doubtless Enron will be used by business schools in the future, but a survey by Transparency International ^{*24} found that transnational corruption had a negligible profile in business school teaching, which is confirmed by our interviews. External issues such as the environment, and some aspects of public protest threats, may appear in social audit and corporate social responsibility courses: but crime externalities do not appear either as a formal category or in substance.

In our view, this is not simply an aberration of education and training. Some of those we interviewed stated their Boards were concerned about social responsibility and sustainability in the community. However, the majority stated that in their experience, concern about crime other than those committed directly against the business was negligible. Except in areas where it was difficult to recruit staff, retail

staff and call centre staff were not given any particular protection (for example on their way to and from work). Even practical action to deal with worry about robberies and post-trauma counselling were on the wane rather than on the increase. In the hi-tech areas, time from idea to market was at a premium, and the building in of crime prevention measures – even crime against the business, but especially secondary crime opportunities that affected purchasers but not sales – was very low down the list of priorities. Furthermore, in regulated industries other than financial services, the regulations related to price and performance, and there was no legal obligation to concern themselves with secondary crimes, so this would simply not get done.

Looked at from the perspective of pure capitalism, unless (as in some cases) Directors develop personal visions or obsessions about social capital in one form or another, it is difficult to argue that they will do anything that is not required by law unless the actuality or risk of crime unequivocally reduces shareholder value. The sheer busy-ness and global involvements of senior executives which makes it much more difficult than a decade ago to get them round a table for a significant period of time, plus problematic profits of traditional industry ‘social responsibility’ leaders such as BT Cellnet (in telecoms) and Marks & Spencers may militate against longer-term social visions. We therefore are fairly sceptical about most companies’ willingness to take action to reduce crime risks unless they are at least fairly cost-neutral or unless provided for in law or regulations.

In this sense there is an expectations gap between those who see plcs having a wide set of stakeholders (employees, customers, the general ‘social interest’) and those who see it essentially as driven by its current company law stakeholders – the shareholders. Some of these issues have been addressed in the recent review of company law, [*25](#) but to the extent that the gap currently is being filled, this is due to the personal ethical and public relations visions of individual executives or Boards, or due to the social pressure exercised via the media. ‘Naming and shaming’ might be one way forward for environmental and money laundering crimes committed by those businesses that are able and intend to continue trading – and the eventual publication of the car theft index is a good example applied to crime-proneness - but we see limited potential for naming and shaming when applied to crime against business lest this simply deter the improved awareness of risk within companies. [*26](#) This is not to provide a complacent portrait of crime risk management in the corporate sector. We encountered cases in which companies were addressing crime risks in a short-term, investment-minimising way that seemed to us to represent sub-optimal cost-benefit analysis for the firm, though this was very unlikely to generate catastrophic failure. In parts of the insurance industry, for example, the attitude appeared to be fraud risks are difficult to identify and the focus should be on ensuring that premium income exceeds outgoings: converting widely distributed IT legacy systems to run internal or outsourced software programmes to enable better fraud risk management was regarded as too expensive and too great a burden for already stretched IT departments. [*27](#) But in the absence of hindsight, there is seldom a single, readily pre-digested path that defines what is and is not a rational approach to Turnbull requirements in relation to crime.

[*24](#) Global Corruption Report, 2001, Berlin: Transparency International.

[*25](#) The Company Law Steering Group (2001) Modern Company law for a Competitive Economy, London: DTI.

[*26](#) Perverse effects are commonplace, but penalising improved identification of crimes against the business would incentivise maximising the dark figure of unidentified crime, e.g. as bad debt. It might make sense to require companies to report frauds they identify, but this would not solve the problem of how to identify fraud, nor are the police in a position to service the reports if made, unless largely for crime analysis and reduction purposes, as currently happens with important collective bodies such as CIFAS (for credit and insurance frauds), the International Chamber of Commerce (for maritime piracy) and the various software and music/entertainment anti-counterfeiting bodies.

[*27](#) This applied to banking as well as to insurance, and probably in other sectors as well. Scarce skills and predetermined budgets can generate absolute constraints on flexible crime risk management.

In our view there is a need for the position of the three key players – government, the police service and businesses themselves – to be examined, in order to be clear which are ‘problem owners’ and which are ‘problem evaders’.

1. Government. The Home Office has never seen business related crime as any kind of priority. It is much more concerned with getting police forces to improve their performance in addressing the crimes that impact directly on the ordinary citizen in their every day lives. The attention given to crimes against business by both Home Office and the police forces is likely to deteriorate over time – if possible – because of the impact on public consciousness of the direct recording of reported incident details. By the same token there will be little desire to include business crime issues in the annual British Crime Survey, which currently excludes all crimes against business and frauds against individuals and the fears/concerns thereof. The fact that the Home Office have carried out only one Commercial Victimization Survey (CVS) in 1994 (covering only the retail and manufacturing sectors) and the absence of the ‘new economy’ from past crime survey analysis is symptomatic. The DTI does not have the Home Office’s contact with police forces and may not wish to be seen as hostile to business in those areas where business generates serious crime externalities and does not seem motivated to do anything about them.
2. Police forces. No crime against business – though terrorism may be *de facto* – are encompassed in Key Performance Indicators or even (other than in the City of London) local force Performance Indicators. Our current and previous research suggests that most forces operate what they might regard as ‘benign neglect’ of both fraud and other business crime problems, with large companies having been ‘granted’ devolved responsibility via their security departments, whether they wish this or not. Similarly SMEs have typically been left to their own devices, or advised to consult websites or – in some sub-types of crime – ‘toolkits’, except where community safety officers take some interest in their crime problems, which our interviews suggest is fairly rare. Very few officers are given any systematic opportunity to understand the security problems facing commerce and industry, and generally business is seen as a resource for funding police and community projects rather than as an object of protection.
3. Business. There are some issues that may be important in Home Office crime numbers terms and in feeding criminal markets, but are below the scale of operations or materiality levels at which Turnbull is pitched. It is helpful to divide businesses into:
 - a. Well-managed businesses who have to decide whether it is cost-effective for them to do something about crime problems they have identified;
 - b. Ill-informed businesses (a linear, not a binary concept) which make little effort to identify problems;
 - c. Sometimes efficiently managed businesses run by domineering CEOs with craven boards and non-executive directors appointed in practice by the CEOs. (This is against Turnbull recommendations but quite possible under existing rules, Enron-style). These businesses may engage in massive false accounting ‘for the firm’ or for sub-units personally, and also in transnational (and perhaps national) bribery;
 - d. Well-managed firms who are aware of their crime business risks and manage them competently, but have no problems about producing items that are easily stolen or converted for criminal use, etc., since these externalities produce no harm for the business itself. They are therefore outwith the

Turnbull or other formal private sector principles and such businesses are not compelled by law to take remedial action. This category could be merged into (a), but there may be differences in tone or degree, depending on how much social acceptability is craved by the Board and how much pressure is put on by the media, politicians or relevant consumer pressure groups.

All of these present different crime communications problems. Many security risks arise as an unintended and unforeseen outcome of the complexity of huge electronic systems meshing together. The most difficult is the pure 'social responsibility' case, in which products – mobile phones are merely the most recent example, with CD burners, twin videos, and easy-to-hotwire cars earlier ones – are produced with little regard for their proneness to be stolen, or used fraudulently or to assist in counterfeiting. There are only two cases where government has taken pre-emptive action. One was in pushing car manufacturers to introduce the steering column lock: an innovation that had a very marked impact on the theft of vehicles so fitted (although in initial years thieves simply targeted those without these locks). The second was the (relative, despite recent rises) success of payment card prevention where, with a propitious combination of falling profits, rising proportion of fraud to turnover, a useful independent research report (!) and high-level ministerial intervention generated rapid change. ^{*28} The pressure being currently exerted on the mobile phone industry to render stolen phones unusable may well, in time, provide a third example. The essence of this strategy is to inject a different dimension into market pressures, in the form of 'government at a distance'.

It was clear from our interviews with businesses that not much regard would be paid to such considerations unless they were compelled by law (as they have been in relation to money laundering) or were similarly the subject of sustained government and/or media pressure, which threatens the brand or even the industry. ^{*29} An e-mail survey carried out on behalf of this study by the Institute of Management Consultants suggested a low level of routine Board-level interest in consultancy on crime-related issues even where the company was the direct victim, and even more so when the company was an unintended facilitator of crimes committed elsewhere. ^{*30} Reputational damage as a motivator is a pure market concept unless it is allied to regulatory powers (as in FSA and other regulated bodies) and/or criminal liability, though global branding generates some greater vulnerability provided the media and business-relevant public care sufficient about an exposed action and sustain their interest.

The extent to which businesses should *and do* take account of crime is unknown in formal representative sample terms; and certainly, modest degrees of fraud and other crime are unlikely to attract media or governmental attention. ^{*31} Nor, with some exceptions, are the mechanisms for identifying fraud (as contrasted with bad debt) well developed in many organisations. ^{*32} As the British Retail Crime Surveys acknowledge, the apportionment of retail losses between customer and staff theft is an art rather than science, but even the BRC surveys do not specifically include management fraud. Factors in the external environment – for example regulations restricting the right of management access to office telecommunications data – can also make risk assessment and management harder.

The domineering chief executive should not be allowed to get his way under corporate governance principles, but we and those we interviewed were deeply sceptical about whether the governance system actually guarantees protection, even though greater professionalisation of non-executives is welcome. Such a CEO might clamp down tightly on employee theft, but loose and manipulative styles of accounting generate opportunities for others, and the Maxwell-style CEO might even offer temptations to those lower down the line to buy their loyalty or silent complicity.

^{*28} See M. Levi and J. Handley (1998) *The Prevention of Plastic and Cheque Fraud Revisited*, London: Home Office Research Study 182; and (2002) *Criminal Justice and the Future of Payment Card Fraud*, London: IPPR. Barclaycard is currently the only payment card business of which we are aware with transparent fraud and profit data, card fraud currently representing approximately 9% of

profits, indicating the risk to the business of fraud left untrammelled. The card industry investment of approximately £1.1 billion in the roll-out of chip-enabled payment cards represented a very expensive piece of crime risk-management which, in our view, has been justified by the accelerating rate of counterfeiting since the decision was taken to make the investment. Had card fraud not increased at a rate of £100 million a year, this might have been viewed in hindsight as a poor risk-management decision, though it might have been fudged as 'integrity assurance' for trust in an intangible industry, etcetera. On the other hand, it would be a mistake to see this as expenditure to reduce the externalities of card crime, e.g. thefts from cars, muggings, etcetera since it was justified on private, not social, cost-benefit analysis.

***29** Identity fraud and e-fraud generally constitutes one area of potential sales or fraud meltdown, with contracts currently charging most losses back to retailers for non-face sales. Public confidence effects are mitigated by fraud protection guarantees by some card issuers (which are relatively cheap, since retailers bear most of the costs) and by visual techniques such as padlocks to indicate security.

***30** Money-laundering is a special case here, since there is a legal obligation to have adequate systems in place and to report suspicions that funds are the proceeds of crime. The survey data are presented in detail in Appendix 1, though we caution that the response rate was poor: 173 usable responses were obtained out of 4,300 members to whom the e-mail questionnaire was sent.

Respondents were asked "Are you aware of any clients (private or public sector) who have given board level consideration to the risks of the business being damaged by crime where...the business itself could be the potential victim of the crime and would be damaged by it. (e.g. fraud, counterfeiting)". Respondent answers were equally split between those who were aware and those who were not aware of the business being the potential victim of the crime and would be damaged by it. (e.g. fraud, counterfeiting).

To a different question of facilitating the crimes against other entities or persons, over two-thirds (67.4%) of respondents indicated that they were not aware of any clients who have given board level consideration to the risks of the business being damaged by crime where the products or services that the business provides could be used for criminal purposes or become a cause of criminal activity. Also, over two-thirds of respondents indicated they had not assisted in giving board level consideration to the risks of being damaged by crime. Just under one-third (31.8%) of respondents answered 'yes' they had been involved in board level considerations to the risks of crime.

***31** Assessing reputational risk partly involves making a judgement about whether anyone in the media will find out or not, either through a leak or as a result of some regulatory or criminal enforcement process.

***32** Some organisations periodically review their bad debt books and examine what proportion of bad individual or corporate debtors have never made a payment or have made the minimum payments followed by default. This is a reasonable proxy indicator of first party fraud.

Bearing in mind these sceptical positions on the possibility of reducing some forms of crime emanating from corrupt or extreme *laissez-faire* corporate cultures, some suggestions for improving the present situation are:

For Business:

1. *Publicity. Make advance plans so that when a major crime causes a substantial and/or sensitive business failure, ensure there is well informed comment on the general nature of the business risk [avoiding the shrinking violet of "it's all sub judice"]*
2. *Wind crime risk management issues into all the business' operating, financial and*

HR systems and approaches, including those such as Investors in People etc.

3. *Train mainstream staff in businesses – not just the accountants - in crime awareness*
4. *Identify risks better and think how much less business you would need to do if you could cut crime costs without sacrificing too much sales: sales that are not paid for are unproductive!*
5. *Share crime data better to develop a better benchmarking of crime (including fraud) risks, and ratchet up the skills levels of internal audit, security and credit control departments including getting them to talk to each other more.*
6. *Industry bodies such as the CBI and IoD could play a significant role as facilitators of benchmarking best practice in business crime reduction, though we appreciate that smaller businesses often feel that they have too much difficulty in just keeping the business running to ‘attend yet another meeting’.*

For Government and Police

7. *Ensure that the subject of business crimes has a real home in the right Department. The Home Office has not actively promoted evidence-led policy on business crime, but has played a key role in ‘encouraging’ some business sectors to design in prevention by publishing risk information. Only the Home Office can influence policing priorities. But the DTI can play an important role via winding director disqualification, company regulation and company law reform into a coherent inter-departmental business crime reduction strategy, while the FSA has a key role in financial crime reduction for regulated firms*
8. *Appreciate that if the police and police authorities do not know about large chunks of crime - those committed against business – they cannot readily fulfil their responsibilities for crime audits and reduction strategies for their areas, nor is it obvious how they can build a proper criminal intelligence model*
9. *Keep up the pressure on the CBI, FSA, the fiduciary professions, etc. over the issues as well as acting as a conduit for their views*
10. *Run PR campaigns and prizes for innovative actions taken by businesses – and perhaps the wooden spoon for most foolish/crass corporate victim, unless that would deter reporting of fraud to the authorities*
11. *Establish a real programme of education and training for the police, alongside people from business, combined with a sense that this work is valued and is part of the core policing function. This should involve regular business-police liaison on the basis of mutual competence and interest [*33](#)*
12. *Establish integrated private sector- police jointly funded initiatives aimed at crime reduction as well as crime investigation: it is the latter that makes most sense to business*
13. *Ensure that the police are aware of the costs that crimes against business impose not just on profits but on amenities for the public – many poor areas are blighted because businesses find it too risky to operate there.*

***33** We are greatly encouraged by the early establishment of an industry liaison officer by the National Hi-Tech Crime Unit, which enables the police to participate actively in an open dialogue with a crucial industry whose products and services have implications for most other businesses. Hi-tech crime has implications for most types of crime, and though our survey has 'relegated' it to specific sub-types such as hacking and computer-related fraud, technology can be used to affect situational opportunities for many types of crime.

Civil Society

- 1. Integrate crime risk management into the business school curriculum, and draw on case studies not just like those provided by Enron, Arthur Andersen and Allied Irish Bank but also by smaller but material-to-SME business cases. The neglect of fraud and corruption issues by many business schools raises serious issues about their preparation of MBAs, not so much on business ethics as a philosophical subject (which is better catered for) but on financial and reputational risk management*
- 2. Encourage shareholder, especially institutional shareholder, and lender pressure in relation to crime risks (a) against the company directly and (b) that can generate reputational risks for the business though the direct victims are outside. Plc directors have to rehearse responses to questions that relevant shareholders or lenders may ask them about. If their crime reduction, crisis response and disaster recovery processes are things they will be questioned about, they have greater incentive to find out what might cause them serious risks.*

In short, in our view there is a need for a rigorous strategy and set of action plans with external performance evaluation, rather than relying on one more document to "turn the corner" against business crime.