Policing fraud in the private sector: a survey of the FTSE 100 companies in the UK

Graham Brooks, Mark Button† and Kwabena Frimpong

(All) Institute of Criminal Justice Studies, University of Portsmouth, PO1 2QQ, UK
†(Corresponding author) Institute of Criminal Justice Studies, University of Portsmouth, PO1 2QQ, UK. Tel: 44 (0)23 9284 3923; Fax: 44 (0)23 9284 3918; email: mark.button@port.ac.uk

Received 15 September 2008; revised and accepted 1 March 2009

Keywords: policing; counter fraud strategies; FTSE 100

Graham Brooks *is a Senior Lecturer at the Institute of Criminal Justice Studies, University of Portsmouth.*

Dr Mark Button *is Associate Head (Curriculum) and Principal Lecturer at the Institute of Criminal Justice Studies, University of Portsmouth.*

Kwabena Frimpong *is a University Tutor at the Institute of Criminal Justice Studies, University of Portsmouth.*

Abstract

Fraud has increasingly become recognised as a problem in the private sector, with a growing number of estimates of the size of the problem produced by official government bodies and private professional services companies such as KPMG. There have, however, been fewer surveys of the strategies being used by the private sector to tackle fraud. This paper presents findings from a survey of the UK's FTSE 100 companies which produced 32 responses and the strategies they are using to counter fraud. It demonstrates a mixed picture of both good and bad practice, when benchmarked against well-recognised standards for tackling fraud, on issues such as having: a strategy; a designated person responsible for fraud; regular risk assessments; preventative measures; investigative resources and effective relationships with the police. It also calls for further research to be conducted on private sector counter fraud strategies.

INTRODUCTION

Fraud is a major cost to society. Levi, Burrows, Fleming, and Hopkins (2007) recently very conservatively estimated that the nature, extent and impact of fraud is in the region of £14 billion (per annum) in the UK alone. This is a substantial figure and one that should register concern with every company regardless of the sector in which it trades. More significantly, around half of the estimated £14 billion mentioned above is lost to fraud in the private sector. The American Association of Certified Fraud Examiners (ACFE) in its 2006 *Report to the Nation*, which only focuses upon 'occupational fraud' (so excludes external frauds) found the median estimate of losses from corporations revenues was 5 per cent, which if replicated across the USA would amount to £652 billion (American Association of Certified Fraud Examiners [ACFE], 2007). The report found that the median loss was $159,000, but nearly a quarter of cases caused losses of at least $1 million and there were nine cases of £1 billion or more! Again, the limitations

International Journal of Police Science and Management,

DOI: 10.1350/ijps.2009.00.0.140

are clear from such a study as it is only occupational fraud and based upon a survey of Certified Fraud Examiners (CFEs). Both of these studies illustrate that in the UK and USA fraud is a major cost to private business. The estimates above come from just two of the numerous studies seeking to estimate the fraud losses of the private sector across the globe (see, eg, KPMG, 2004a, 2004b, 2006; Shury, Speed, Vivian, Kuechell, & Nicholas, 2003).

There have, however, been relatively few studies seeking to examine the counter fraud strategies used by the private sector to police fraud. One of the few is the large professional services provider Ernst & Young, which conducts a global fraud survey every few years and in 2006 published its ninth edition. The 2006 survey included 586 respondents from 20 countries, which included some countries considered to be 'emerging markets' such as Brazil, China, India and Russia (Ernst & Young, 2006). PricewaterhouseCoopers has also funded a major survey of private companies which, although yielding extensive data on fraud, only touches upon the strategies being used to combat fraud (Bussmann & Werle, 2006). In the public sector in the UK there is also an annual HM Treasury survey of public bodies and their counter fraud strategies, but this survey does not cover the private sector or local government (HM Treasury, 2005, 2006, 2007).

The limited research assessing in depth what private companies are doing to tackle fraud suggested that a preliminary study was required. We therefore decided to undertake a survey of the FTSE 100 (i.e., the 100 largest capitalised companies trading on the London Stock Exchange). The aim was to find out what the largest and most successful companies in the UK were doing to tackle fraud. This, if successful, would then provide insights for a wider study into the private sector's counter fraud strategies in the FTSE 250, as well as many small and medium sized enterprises (usually known as SMEs). It was also felt that publication of the results would be timely given the recent recommendations of the Fraud Review (2006) and the changing national counter fraud infrastructure that is emerging as a consequence. The results we present cover 32 responses from the 100 questionnaires sent out. This is a relatively small sample, but we believe, given the lack of detailed data on private sector strategies, that it deserves to be published to stimulate further debate and research of the private sector approach to policing fraud. This paper will set out the methodology used and then examine the results of our survey. Before we embark upon that, however, it is necessary to set out a model counter fraud strategy.

MODEL COUNTER FRAUD STRATEGY

The identification of a model counter fraud strategy is essential to conducting this survey because one of our other aims was to benchmark what the FTSE companies are doing against best practice. For the private sector there is no established benchmark of best practice for countering fraud, whereas in the public sector there have been a variety of best practice guides promulgated by the government and other prestigious bodies. *Managing the Risk of Fraud: A Guide for Managers* (HM Treasury, 2003) and *Good Practice in Tackling External Fraud* (National Audit Office & HM Treasury, 2004) are examples from central government. The Chartered Institute of Public Finance and Accountancy (CIPFA) (2006) has also contributed to the development of best practice with its document *Managing the Risk of Fraud Actions to Counter Fraud and Corruption* (which in turn was heavily influenced by the National Health Service (NHS) model which started in 1998). The model used in the NHS is also considered to be best practice given the impressive results returned by the NHS Counter Fraud and

Security Management Service (CFSMS), which has brought a 12 to 1 return on investment, saving £811 million for the NHS (NHS CFSMS, 2007a). (There was other research published prior to 2007 which also indicated the high return on investment (see NHS CFSMS, 2003).) However, for the sake of clarity, if we distil the best practice from the above we are left with some of the following strategies:

- designating a person with responsibility for counter fraud strategy
- the possession of a counter fraud strategy
- measurement of fraud on a regular basis, including evaluation of counter fraud strategies
- anti-fraud culture strategies such as general fraud awareness training
- fraud prevention strategies
- vetting of staff/contractors in key positions of trust/sensitivity
- independent whistle-blowing mechanisms
- employment of or access to professionally trained counter fraud specialist (CFS)
- effective partnership with other relevant bodies
- pursuit of civil and criminal sanctions against fraudsters
- pursuit of financial redress.

The elements of the above strategies will be considered in more depth in the results section. Before we embark upon that, we will set out our methodology.

METHODOLOGY

In order to assess the level at which the private sector considers fraud an important issue, we decided to undertake a postal survey of the most successful companies in the UK in the FTSE 100. As these are the largest, complicated and most successful companies, one would expect there to be counter fraud strategies in place. Therefore, in November 2006 we sent 100 questionnaires to the companies in the FTSE 100. The questionnaire contained both open and closed questions, was accompanied by a letter and was directed at the chief executive, with a request to pass it on to the person with responsibility for countering fraud. We informed the recipients of our questionnaire that we had set a deadline date of January 2007. Reminder letters were sent in the hope of increasing our response rate as we closed in on our deadline date. In total, we received 32 responses. This is not a substantial response rate. However, since we only set aside three months in which to respond to our questionnaire, our response rate of nearly one-third is a promising return. Our survey reflected the elements of a model counter fraud strategy mentioned earlier with questions seeking information from companies on what they were doing in each of those areas.

There are of course limitations to this research. Basing a paper on 32 responses provides only a limited foundation, but it was felt that the findings warranted publication to stimulate further research and debate in an area in which there has been very limited academic interest. It is also difficult to operationalise and define such a slippery term as fraud. For example, as illustrated by Doig (2006, pp. 19–21) fraud is associated with a range of orthodox activities; it is about deception, it is careless, reckless behaviour and/or is carried out with criminal intent. Rather than specifically define fraud and restrict the responses open to us, we took the decision to enable respondents to decide what they considered constituted fraud. The expectation was this 'open' approach would secure a wide response. One of the consequences of this was that most companies made limited reference to key financial reporting controls such as the (US) Sarbanes-Oxley Act, which we would have expected.

RESULTS

As we mentioned earlier, we received a total of 32 responses out of the questionnaires sent. In this response there are a number of different companies working in different sectors of the business world. The approximate annual revenue of those that responded ranged from £249.2 million to more than £132 billion, with some employing more than 400,000 staff. Table 1 below illustrates the different sectors which the 32 respondents were from. It shows the two biggest groups were manufacturing and banking/finance, accounting for just over 40 per cent. With such a range in revenue and employees and size of company, the seriousness and consideration given to counter fraud measures also differed markedly.

Counter fraud strategy

One would expect any large organisation to have some type of strategy to counter fraud, given the large number of studies illustrating the potential size of the problem. Of the 32 responses, 18 claimed to have a counter fraud strategy, ten were without a strategy and one admitted it was unaware either way; the rest (3 companies) did not answer. Given that, in the financial services sector, the regulator, the Financial Services Authority, mandates minimum standards for addressing financial crime and money laundering, just under a third of the 18 (the five financial services companies that responded) had to have a strategy and this illustrates the poor commitment to this approach amongst the wider FTSE 100 respondents. Part of any counter fraud strategy is assessing the effectiveness of the approach taken. This can range from a review with audit, a measure of how vulnerable a company is to fraud, to regular production of management information such as statistics, and assessment and analysis of cases investigated and what is learnt from them.

A few of the following responses clearly illustrate the range of counter fraud strategies employed by those companies in the FTSE 100. One company claimed that:

> Actual and attempted fraud instances are collated and logged. In this way levels of fraud are kept under constant review (FTSE100Q8[1]).

However, perhaps less systematic than above, one company claimed:

> We undertake fraud vulnerability assessments where appropriate and 'regular management information is produced' reflecting the range of counter fraud strategies employed (FTSE100Q15).

Furthermore, another company stated that it had:

> Regular Sarbanes-Oxley testing of key financial reporting controls; internal audit reviews of the adequacy of fraud risk management across the Group (FTSE100Q31).

Designated person

Of the 32 responses, 26 had a designated person responsible for counter fraud and 6

Table 1: Responses by sector

Organisation	*Responses*
Transport	2
Telecoms	2
Construction	4
Consumer goods	3
Natural resources	3
Manufacturing	4
Services	4
Retailing	3
Energy	2
Banking and Finance	5
Total	32

were without a specific designated person. Across the FTSE 100 companies which responded to our questionnaire, there was a wide range of job titles and reporting structures for those considered to be the named responsible person for counter fraud. These ranged from Counter Fraud and Forensic Accounting Officer, Director of Fraud, Financial Crime Manager and Head of Audit and Operational Risk, to Head of Loss Prevention and Security, Head of Profit Protection, Head of Compliance and Director of Audit.

While some companies had a specific named person to deal with counter fraud, in others it was indicated that counter fraud was a shared responsibility, which seemed to fall to the Head or Director of Risk or Security in the company. In one company, counter fraud appeared to be shared amongst a number of employees with no clear indication to who was responsible for counter fraud. This has to be considered an unsatisfactory approach. A clearly designated person whose remit is to deal with counter fraud issues is an essential element of a successful counter fraud strategy. After all, with a clear remit and knowledge of fraud such a person could be a conduit to broadcast fraud issues in a company and raise awareness, prevent fraud, develop an anti-fraud culture and work and liaise with the police or Serious Fraud Office if required, and produce a report for the company board. From our results it also appears that there is a variety of reporting structures in place. Similar to the above mentioned approach, counter fraud issues can be reported to a Chief Executive, Finance Director, Head of Risk or Security or Chair of the Audit Committee.

Risk assessments

Of the 32 responses, 27 companies indicated that they had some type of fraud risk assessment, 3 responded that they had no risk assessment and 1 worryingly had no idea if it had any risk assessment at all. While this is of some concern, more worrying is the frequency at which a fraud risk assessment is undertaken. From our responses a few of the companies stated that fraud risk assessments are an ongoing process. We too would suggest that this is the most appropriate approach to use to counter fraud. This is emphasised here since without continuous assessment it is possible that a culture and acceptance of fraud might develop. Further responses showed that some companies indicated that they undertook a risk assessment monthly, some quarterly, bi-annually, annually, and periodically (eg, 1–3 years). Fraud is an ongoing problem, which needs continuous monitoring and assessment. For a counter fraud strategy to be successful, regardless of the risk assessment strategy in place, the frequency of the assessment is of paramount importance.

In addition to this, some of our responses indicated that fraud risk assessments were dependent on the type of risk, eg, fraud in or from a foreign country (see Ernst & Young, 2006) and/or company with which the FTSE 100 company will deal, and the introduction of a new company product. It is hoped, however, that before any new product is introduced to the market, eg, a specific financial product, a manufactured product (chemical or industrial) or one of personal identification, all aspects of fraud would be considered.

Prevention and anti-fraud culture

Screening a new employee, contractor and/or supplier is also an important part of the preventative aspects of a counter fraud strategy. However, for a counter fraud strategy to be successful, screening of employees, contractors and suppliers should be ongoing. The approach taken regarding employees and risk assessment is interview, reference checks, credit checks and requesting original documentation such as qualifications etc. For contractors and suppliers

it appears from our survey that they are assessed for a conflict of interest, and checks are made on VAT numbers and similar specific identifiers, combined with a credit reference and Companies House search. It was also noted that many of the FTSE 100 companies kept and reviewed their lists of contractors and suppliers. From the information we have received, it appears that, if a FTSE 100 company is working in partnership in some capacity with another company that is under contract and providing a service, a far more extensive risk assessment is undertaken than if directly employed by the company. Their customers, stakeholders and partners are left in no doubt as to how serious the matter of fraud is for some. For example, one company made it explicitly clear when saying:

> We try to regularly improve our customer vetting to prevent fraud. We create an anti-fraud culture by issuing strategic communications to key stakeholders in the business (FTSE100Q18).

This is perhaps understandable since the company purchasing a service should make sure that it is getting the service it has requested and is paying for and that it is a creditable company to do business with. However, this can also be said of its own employees. Full-time employees commit a substantial amount of fraud (BDO Stoy Hayward, 2008; Ernst & Young, 2003; Gill, 2005; Hollinger & Davis, 2006; KPMG, 2007), and yet, from our survey, it appears that there are far more stringent and comprehensive risk assessments undertaken regarding 'external' companies and their employees than those 'internal' employees who are familiar with their company, its practices, methods of operation etc.

Developing an anti-fraud culture is considered a major part of a preventative strategy. One of the tools used to achieve this is various forms of staff training. Of the 32 responses we received, 21 had 'general staff training'. This general training appeared to revolve around raising the awareness of counter fraud issues. For example, some of the responses we received regarding this matter are comprehensive. One respondent stated:

> Embedded control procedures including fraud policy and whistleblowing procedures, code of conduct and induction (FTSE100Q4).

While another FTSE 100 company had a clear established approach where:

> There is a published Anti-Fraud policy. We also deliver fraud awareness training and issue fraud awareness bulletins (FTSE100Q12).

It was pleasing to see that 31 of the 32 responses stated that they were actively pursuing measures to prevent fraud and create an anti-fraud culture; only one company indicated that it was not in the process of developing an anti-fraud culture.

The nature and approach taken in developing an anti-fraud culture, however, varied across the respondents. For example, in some companies, all new employees were introduced to the problem of fraud as part of the company induction. In other instances some employees attended an annual finance fraud conference, some were offered the opportunity to update their knowledge and some had specially commissioned packages depending on their line of business. In addition to this varied approach in developing an anti-fraud culture, it also appears that all employees were trained when specific frauds or a series of frauds were discovered. Although this is laudable, our concern here is that preventative measures should already be part of a counter fraud strategy. While we are aware that it is

impossible for every company to predetermine every type of fraud it might encounter, it has no excuse for the majority of them. Regardless of its 'business', it must be aware that certain areas of its 'business' are more vulnerable to fraud than others and that the assessment of risk mentioned above is an integral part of developing an anti-fraud strategy and anti-fraud culture.

However, some of the responses we received illustrated that many companies are now beginning to cultivate a clear anti-fraud culture. In response to our survey many companies have made reference to: fraud awareness bulletins, use of the intranet to disseminate information regarding fraud, holding fraud risk workshops to identify potential fraud risks and actions that are needed to counteract them, strict financial control permeating throughout the company and, significantly, the development of specific whistleblowing procedures.

In the final part of this section a note of caution is needed. Any company that takes fraud seriously and has, or is in the process of developing a counter fraud strategy is to be commended. However, the development of an anti-fraud culture is of limited value if employees have no clear direction as to what fraud is, or how it might possibly emerge. A codified set of guidelines regarding fraud, ethical behaviour, a set code of conduct, response plan(s) and anti-fraud policies alone are insufficient. If we fail to educate and hold accountable those who ignore, break or circumvent 'codes of conduct', then our attitude to fraud is unlikely to change. After all, as Ernst & Young (2003) noted, Enron had a code of ethics and a whistleblower mechanism, and yet neither worked. A strategy needs direction and clear codes of conduct, which need to be enforced if it has any chance of success. Issuing a counter fraud policy is the start of a counter fraud strategy: it is not an end in itself.

Reporting fraud

Whistleblowing has gained much greater prominence in the boardrooms of companies with the passage of the Public Interest and Disclosure Act 1998, the publication of the British Standard PAS 1998/2008 Code of Practice on Whistleblowing Arrangements, and the services offered by bodies such as Public Concern at Work. Such measures are advocated for the much wider purpose of exposing wrongdoing, but independent whistleblowing mechanisms also have a very important part to play in a counter fraud strategy. There have been a number of high profile frauds where the mechanisms to expose them have been regarded as weak (Levi, 2006). Frequently, a manager is suspected of fraud by his or her employees, but for them to make allegations against that manager to the manager's superior is often fraught with risk. The manager's superior might be in on the scam or simply dismiss the allegation, leaving the exposing employee exposed. One of our main concerns in the survey was what, if any, processes were in place to report fraud independent of management, particularly internal fraud. If an employee did not want to report a fraud to his or her line manager, many had the option of a hotline or whistleblowing mechanism. For example, one company claimed that it had a:

> Whistleblowing programme, strong disciplinary action, report criminal acts to authorities (police); articles in corporate news; fraud policy (FTSE100Q27).

Furthermore, and perhaps due to emerging markets, another company felt it necessary to have a:

> Whistleblower hotline available globally . . . documented and robust internal control environment; fraud response plan under development; consistent and

vigorous response to incidents (FTSE100Q31).

However, while such statements are encouraging, little information was forthcoming from our survey on the process of whistleblowing and how it should work. A company can claim to have an internal policy and process where employees can raise their concern regarding other employees; however, what advice, protection and support is in place for the whistleblower is of paramount importance. This area is clearly in need of much more research.

Counter fraud specialists

Of the 32 companies which responded to our survey, 17 employed dedicated counter fraud staff, which in total amounted to 160 employees, while 13 had no specialist staff, and 2 did not answer the question. From this information it appeared that 14 provided training for their specific counter fraud staff, 1 company claimed that it did not provide training, 1, worryingly, did not know if it provided training for its staff and the rest did not answer the question.

Furthermore, from the 17 companies which responded to our survey that claimed to have trained counter fraud staff, it is apparent that there is no specific counter fraud qualification recognised by the FTSE 100. This contrasts with the public sector where the Accredited Counter Fraud Specialist (ACFS) has become the norm (Button, Johnston, Frimpong, & Smith 2007). Although one company stated that it had its counter fraud staff trained and accredited by the Counter Fraud Professional Accreditation Board (CFPAB), there were a diverse range of other courses used such as: the Telecommunications United Kingdom Fraud Forum (TUFF), i2 Training, CIFAS Fraud Training, Association of Certified Fraud Examiners (ACFE), a Diploma in Fraud Investigations, the use of qualified external consultants, ad hoc provision from third-party providers and in-house courses and seminars made available to employees.

The variety of different organisations that offer counter fraud courses/training is hardly surprising. As a nascent profession, the counter fraud profession has only recently received the recognition it perhaps should have (Button et al., 2007). Therefore, it appears that organisations in the private sector, unlike public bodies which are represented and involved with the CFPAB, tend to use an organisation that is specifically related to their line of work. This is represented in the types of external and internal fraud investigated by the FTSE 100. The types of fraud range across credit card fraud, embezzlement, theft of a person's identification, cash theft, and misappropriation of assets, theft of company property, salary and payroll fraud, insurance and health care fraud and many others that fall under the broad canopy of fraud.

Cooperation and sanctions

It appears from our survey that cooperation with other companies during a counter fraud investigation is limited. Of the 32 respondents 19 claimed that they had worked with or had recourse to liaising with another agency in the course of an investigation, with one company clearly stating that it did not work with anybody else. The rest did not respond to the question regarding cooperation. As we would expect if any cooperation, collaboration or advice were required, law enforcement organisations such as the police, Serious and Organised Crime Agency (SOCA), the majority of our 19 respondents contacted HM Customs and Revenue and the Financial Services Authority (FSA). While other investigative bodies such as the Telecommunications UK Fraud Forum and those

involved in the world of finance and insurance depending on the circumstances of the crime, were contacted, it appears that the company that has knowingly experienced fraud can draw on a range of different organisations and sanctions to 'punish' or discipline the offender(s).

Once an investigation has reached what we might refer to as the 'sanction stage', then it appears that the seriousness of the fraud seems to be the main factor in deciding what type of sanction should in fact be pursued. This is perhaps similar to the evidential and public interest test that the Crown Prosecution Service uses to judge whether a case should go forward. The difference here, however, is that the company, perhaps alone or possibly in conjunction with the police, might prefer to use internal procedure and 'discipline' the offender without recourse to the criminal law. Indeed, one of the findings from Bussmann and Werle's (2007) global survey was that only 51 per cent of internal and external perpetrators of economic crime were charged in the criminal courts.

It is debatable, however, to what extent a public prosecution will be pursued by the private sector, particularly maximum deterrence with recourse to the criminal justice system. After all, a private sector company would generally rather deal with fraud privately than risk public exposure (Doig, 2006; Gill & Hart, 1997; Levi, 1987). Regardless of this, no company will accept a small percentage of the estimated loss mentioned at the start of this paper — £14 billion — without some kind of restitution. Consequently, the range of sanctions used across the FTSE 100 to resolve a matter of fraud might be categorised in the following ways: dismissal without sanction, internal disciplinary procedure, suspension for a period of time, closure of accounts, notification of offender to credit reference and fraud prevention agencies, recovery of all assets/money where possible and, ultimately, criminal prosecution.

The relationship with the police

Once the company has decided it wants to initiate criminal proceedings, depending on the seriousness and severity of the fraud committed, it has to contact the relevant law enforcement agency. In this case it is primarily the police. Given that past research has suggested a lack of police interest, we sought to discover if this also applied to FTSE 100 companies (Levi, 1987, 2003). We therefore asked to what extent those detected cases of fraud were actually passed to the police to initiate the prosecution process. From our survey the breakdown of information is as follows: 9 out of the 23 responses stated that all cases of detected fraud (100 per cent) were sent to the police, 2 companies claimed that this happened 90 per cent of the time, 1 company suggested that it happened approximately 80–90 per cent of the time, with another company clearly saying its cases were sent to the police 80 per cent of the time. Furthermore, 2 companies claimed they sent the cases to the police less than 50 per cent of the time, with another company qualifying this by saying that it was dependent on the 'police' region. Even more worrying is that 1 company sent its cases less than 10 per cent of the time, 1 sent them around 5 per cent of the time, one claimed that it was insignificant, 3 had no idea if a case had been sent and 1 claimed that it did not matter as fraud was detected prior to provision (opening) of the account.

This low level of police contact is worrying. However, some of the responses we received clearly answered our concern. For example, one company said that:

> The police are particularly unresponsive and uncooperative (FTSE100Q7).

Other FTSE 100 companies appeared to concur with this view claiming that:

> Police not interested in frauds of less than £100K!! Poor response generally! FTSE100Q10.

> Police do not appear to take cases of 'minor' fraud seriously. You have to prepare the case for the police, ie evidence, etc, without this, they [the police] are not too interested in a minor offence (FTSE100Q11).

> Anecdotal evidence suggests a low likelihood of police involvement in fraud below £100K in the UK. Crown Prosecution Service adds another layer that may still lead to no prosecution (FTSE100Q20).

There was also other evidence to suggest a good response from some police forces. One respondent claimed:

> We receive strong support from Northumbria Police (Local Force Area) in all cases referred to them. Cases referred to other force areas have not always received the same level of commitment (FTSE10012).

Yet another company in the FTSE 100 applauded the way in which the police dealt with fraud:

> City of London Police excellent; Lothian and Borders Police excellent; Metropolitan Police, very good; West Midlands very good. The rest leave a lot to be desired (FTSE100Q26).

It is understandable that the City of London Police are considered excellent with their record on responding to fraud; it is less evident why, and with such a geographical spread, Lothian and Borders Police and the West Midlands Police are thought of so highly too. It appears from the data that there is no clear pattern across all police forces of their attitude to fraud. With such a mixed approach it is difficult to draw a conclusion. However, what is apparent is that the relationship or impression of the police from the FTSE 100 respondents is that they range from 'particularly unresponsive and uncooperative', with a reluctance 'to take on business crime' to 'not interested if minor offence'. It also appears though, that some police forces are excellent, such as the City of London, the Lothian and Borders and also the Northumbria Police, and positive feedback was provided on the response of the Metropolitan and West Midlands Police.

There also seemed to be some disappointment with the lack of resources that the police had to deal with fraud issues, which led to comments such as:

> In the UK the Police will not undertake major fraud on our behalf. They require the evidence to be provided to them once we have undertaken our own investigations (FTSE100Q21).

Furthermore, this same company continued to make an interesting point, one that clearly illustrated the global nature of fraud and the problems which a company, no matter how powerful, will encounter as it seeks out new markets. The company stated that:

> Also, because . . . PLC operates across the world . . . in many third world countries there is no fraud investigation capability by the local police. Corruption is so rife we are often compelled to apply preventive measures and then take no further action (FTSE100Q21).

Conclusion

The policing of fraud in the UK's largest companies provides a mixed picture. From this small survey it is clear that, of those companies in the FTSE 100 that responded to our questionnaire, there are some with sound counter fraud strategies and procedures in place, but there is also evidence

of significant gaps in the counter fraud strategies as judged against benchmark strategies. The possession of a counter fraud strategy, regular fraud risk assessments, the promotion of anti-fraud cultures, reporting mechanisms and full use of sanctions were all found to be wanting in many of the respondents. Clearly this is a relatively small survey and further research is required, not just on the FTSE 100, but reaching out to the wider private sector and particularly SMEs. This and future research should be used to inform further developments in the promotion of best practice, that is much more influenced by the needs of the private sector in policing fraud. Given that one of the major recommendations of the Fraud Review was for a National Fraud Strategic Authority to develop a national counter fraud strategy, which is now coming to fruition, one of its priorities will clearly be to secure further information on the extent and quality of counter fraud strategies in the private sector and to identify a model strategy, which is then actively promoted (Attorney General's Office, 2008; Fraud Review Team, 2006). If the evidence from this small survey is typical of the private sector, there will be much work to do, but also many rewards to be reaped in more effective counter fraud strategies that reduce the cost of fraud to society.

Note

1 All responses following are accompanied by an indication of the specific question in the survey instrument (ie., FTSE100 Q8) indicating question 8 in that document.

References

American Association of Certified Fraud Examiners. (2007). *2006 ACFE Report to the Nation*. Retrieved January 28, 2008 from http://www.acfe.com/documents/2006-rttn.pdf

Attorney General's Office. (2008). *About the National Fraud Strategic Authority.* Retrieved January 12, 2009 from http://www.attorneygeneral.gov.uk/NFSA/NFSA%20-%20About%20the%20NFSA.pdf

BDO Stoy Hayward. (2008). *Fraud Track 5 Summer 2008 Update.* UK: author.

Bussmann, K. D., & Werle, M. M. (2007). Addressing Crime in Companies: First Findings from a Global Survey of Economic Crime. *British Journal of Criminology, 46*, 1128–1144.

Button, M., Johnston, L., Frimpong, K., & Smith, G. (2007). New Directions in Policing Fraud: the Emergence of the Counter Fraud Specialist in the United Kingdom. *International Journal of the Sociology of Law, 35*(4), 192–208.

Chartered Institute of Public Finance and Accountancy. (2006). *Managing the Risk of Fraud*. London: author.

Doig, A. (2006). *Fraud*. Devon: Willan Publishing.

Ernst & Young. (2003). *Fraud: The Unmanaged Risk. 8th Global Survey.* South Africa: author.

Ernst & Young. (2006). *9th Global Fraud Survey.* Retrieved January 28, 2008 from http://www.ey.com/Global/download.nsf/Ireland_EOY_E/Thought_Leadership_ Fraud_Survey/$file/EY_Fraud_Survey_June2006.pdf

Fraud Review Team. (2006). *Final Report*. London: The Legal Secretariat to the Law Officers.

Gill, M. (2005). *Learning from Fraudsters*. Leicester: Perpetuity Research and Consultancy International.

Gill, M., & Hart, J. (1997). Exploring Investigative Policing. *British Journal of Criminology, 37*(4), 549–567.

HM Treasury. (2003). *Managing the Risk of Fraud: A Guide for Managers.* London: author.

HM Treasury. (2005). *Fraud Report 2004–05: An Analysis of Reported Fraud in Government Departments*. London: author.

HM Treasury. (2006). *Fraud Report 2005–06: An Analysis of Reported Fraud in Government Departments*. London: author.

HM Treasury. (2007). *Fraud Report 2006–05: An Analysis of Reported Fraud in Government Departments*. London: author.

Hollinger, R. C., & Davis, J. L. (2006). Employee Theft and Staff Dishonesty. In M. Gill (Ed.), *The Handbook of Security* (pp. xx-yy). Basingstoke: Palgrave.

KPMG. (2004a). *Fraud Survey 2003*. Retrieved January 28, 2008 from http://www.kpmg.com/aci/docs/surveys/Fraud%20Survey_040855_R5.pdf

KPMG. (2004b). *Fraud Survey 2004*. Retrieved January 28, 2008 from http://www.kpmg.com.au/aci/docs/Fraud-Survey-2004.pdf

KPMG. (2006). *Fraud Survey 2006*. Retrieved January 28, 2008 from http://www.kpmg.com.au/Portals/0/FraudSurvey%2006%20WP(web).pdf

KPMG. (2007). *Profile of a fraudster. 2007 Survey*. Retrieved August 15, 2008 from http://www.kpmg.co.uk/pubs/ProfileofaFraudsterSurvey(web).pdf

Levi, M. (1987). *Regulating Fraud*. London: Tavistock Publications.

Levi, M. (2003). Organised and Financial Crime. In T. Newburn (Ed.), *Handbook of Policing* (pp. 443–466). Cullompton: Willan.

Levi, M. (2006). The Media Construction of Financial White Collar Crimes. *British Journal of Criminology, 46*, 1037–1057.

Levi, M., Burrows, J., Fleming, H., & Hopkins, M. (2007) *The Nature, Extent and Economic Impact of Fraud in the UK*. London: ACPO.

National Audit Office and HM Treasury. (2004). *Good Practice in Tackling External Fraud*. London: author.

National Health Service Counter Fraud and Security Management Service. (2003). *Countering Fraud in the NHS: Protecting Resources for Patients. 1999–2003 Performance Statistics.* London: author.

National Health Service Counter Fraud and Security Management Service. (2007a). *Countering Fraud in the NHS: Protecting Resources for Patients. 1999–2006 Performance Statistics*. London: author.

Shury, J., Speed, M., Vivian, D., Kuechell, A., & Nicholas, S. (2003). *Crime Against Retail And Manufacturing Premises: Findings From The 2002 Commercial Victimisation Survey.* Retrieved January 23, 2008 from http://www.homeoffice.gov.uk/rds/pdfs05/rdsolr3705.pdf