

The importance and difficulties of researching into fraud

Dr Andrew Higson

The Business School
Loughborough University
Loughborough
Leicestershire
LE11 3TU, UK

E-Mail: A.W.Higson@lboro.ac.uk

Web: <http://www.accounting-research.org.uk>

Phone: 00 44 1509 223104

The importance and difficulties of researching into fraud

Over the past decade commercial and technological developments have revolutionized the business world. Whilst the existence of fraud may be as old as time, these developments have created new threats to organizations. The internet has provided the basis for cybercrime - and cyber terrorism is only one step beyond this. At such a time, the importance of research into security issues should not be underestimated.

Keywords: Fraud, cybercrime, corporate governance, research.

Introduction

Recent financial scandals have highlighted the destructive impact of fraudulent behaviour. The collapse of a large company not only affects its shareholders and employees, but also suppliers, customers, banks, stock markets and pension funds. However, most frauds are not cataclysmic – indeed, it could be argued that most frauds are not discovered. Traditionally the most serious forms of frauds were perceived as originating from within an organization (by senior management and other employees of an organization maybe in collusion with third parties). Technological developments are now making organizations increasingly vulnerable to fraudulent activity from outside. Given the rapid expansion of the internet and the interconnectivity that it creates, it is not surprising that cybercrime is on the increase - but what makes this type of crime different is that there may be no limit to its potential destructive impact.

Given the current dynamic business environment, this paper argues that it is imperative to conduct research into, and educate managers about, the dangers arising from the threat of fraud. A major problem is that fraudulent behaviour, by its very nature, tends to be covert. The paper commences by examining various definitions of the word “fraud” and the difficulties of identifying something as a “fraud”. These sections are developed from earlier work (Higson, 1999, 2002a, 2002b). The paper then examines the increasing threats from cyberfraud and cybercrime – and emphasizes the directors’ responsibilities for establishing a system of controls to protect their businesses from these developments. There is then a discussion of the importance of researching into fraud, arguing that the evolving nature of the subject may mean that the approaches taken may have to differ from those of traditional academic studies.

What is fraud?

Huntington and Davies (1994, p.3) point out that “English law does not define fraud”, but based on Buckley J’s comments in *Re London and Globe Finance Ltd*, they considered that any fraud would have two essential elements, namely, deception or concealment, and deprivation or loss to the victim. This is in line with French’s (1985, p.128) definition of “fraud” as: “Deception, either by stating what is false or by suppressing what is true, in order to induce a person to give up something of value.” Comer (1985, p.439) considered it to be “[a]ny behaviour by which one person intends to gain a dishonest advantage over another”, and that “[a] fraud may not be a crime”. This would seem to be a somewhat wider interpretation of the meaning of the word “fraud”. In terms of external auditing, the Auditing Practices Board’s (APB, 1995) Statement of Auditing Standards (SAS) 110 (para.4) viewed fraud as comprising of “both the use of deception to obtain an unjust or illegal financial advantage and intentional misrepresentations affecting the financial statements by one or more individuals among management, employees, or third parties”. It considered that fraud could involve:

- falsification or alteration of accounting records or other documents,
- misappropriation of assets or theft,
- suppression or omission of the effects of transactions from records or documents,
- recording of transactions without substance,
- intentional misapplication of accounting policies, or
- wilful misrepresentations of transactions or of an entity’s state of affairs. (APB, 1995, para.4)

As there is not a criminal offence of “fraud” in English law, any prosecutions have to be brought against a specific offence - “the most common being theft under s1 of the Theft Act 1968, obtaining property by deception under s15 of the Theft Act 1968, and false accounting under s17 of the Theft Act 1968; carrying on business with the intent to defraud under s458 of the Companies Act 1985 and the

common law offence of conspiracy to defraud” (Huntington and Davies, 1994, p.3). It can, therefore, be seen that the word “fraud” is commonly used as an umbrella term to cover a multitude of offences which may differ markedly in size, e.g. they can be very small (e.g. a false expense claim) or very large (e.g. a fictitious overseas subsidiary). Whether all of these should be classified in the same way is problematic.

Another problem relates to the actual identification of something as a “fraud” (e.g. Levi, 1987). It is conceivable that victims may not even realise what has happened. Indeed, the classification of an action as being fraudulent may depend on the motivation behind it (e.g. was it deliberate or accidental?). Burns (1998, p.38) asked: “At what point does sharp practice become fraud?” This does seem to imply that the dividing line between the two, in certain circumstances, may at the very least be very fine. Therefore, “[a]s fraud is the product of deception, it follows that estimation of its incidence is subject to significant error, with the true but unknown extent of fraud greater than detected fraud” (Oakes and Standish, 1996, p.2). In terms of fraud, between black and white there is a very large grey area; for example the manipulation of results or the timing of sales (to achieve a bonus or promotion) are not stealing but would be misleading. Consequently, many companies may not see these things as fraud - unless there is the taking of “cash” it tends not to be viewed as fraud. Also, the dividing line between fraud and business misjudgement may often be indistinguishable - a product may be a loss leader, and would not be classified as a fraud. Another problem is that what is a fraud in one decade is not one in another decade and a whole range of activities are often not seen as frauds.

SAS 110 (para.3) points out that: “It is for the court to determine in a particular instance whether fraud has occurred.” This emphasises the importance of remembering that until a case has been proven, one is dealing with suspicions and allegations of fraud (see Table 1).

Table 1
The Anatomy of a "Fraud"

- 1) A deception/misappropriation occurs.
- 2) An anomaly is discovered.
- 3) The suspected perpetrator/s is/are identified.
- 4) Evidence is gathered.
- 5) The matter is reported externally.
- 6) The evidence is strong enough to support a prosecution.
- 7) The perpetrator/s is/are found guilty of committing a crime.

There is a view that the vast majority of small frauds are probably not discovered. Elliott (2000, p.33) reinforced this point: "No frauds discovered does not mean they do not exist or could not easily occur. Those organisations which fail to recognise this are also most likely to fail to act appropriately when a fraud is suspected or discovered."

It is important to follow up suspicions. Often a fraud is not seen to be a fraud at the outset - by its very nature someone has tried to cover up something. Therefore, when something comes to light it may be described as "an accident", "an error", "incompetence", "normal", "the computer always does this", "a virus", etc. These occurrences should be investigated - they may be perfectly innocent, but they may also be hiding something more sinister.

If something untoward is suspected, a common response may be denial and then anger and then a desire to get even. However, it is necessary to understand what has happened before any direct action is taken – this needs to be done discreetly, but damage limitation must also be considered. The evidence and the system need to be secured. It is necessary to be careful about accusing the wrong person – claims for wrongful dismissal are not unknown. It is important that managers understand their legal position. If the managers are unable to prove something they could well be facing legal action for constructive dismissal. When a fraud is suspected a business should take proper legal advice. If the fraud has cost the business a lot of money, the cost of taking legal advice will pale into insignificance. When the situation has been clarified, the

suspected person could be approached and then appropriate action taken. It must be borne in mind that if only one person out of a team of three is confronted, the other two people could destroy the evidence.

In order to construct a strong case the quality of the evidence is critical, however crucial evidence may not be captured (e.g. loss of trail) or crucial evidence may become inadmissible (e.g. the evidence has been tampered with). Another problem is that collusion may make it difficult to prove what has happened, therefore, imprecision regarding the amount involved and when the fraud actually occurred, may undermine any attempt to take the matter further. The identification of weak internal controls may result in difficulties in making a convincing case. Therefore, management need to make a judgement as to how much effort should go into an investigation and assess the cost/benefit relationship of taking the matter further.

The obligation to report fraud is not particularly clear. The view may be taken that the identification of a suspected fraud was nothing to do with the outside world, hence the reason it may not be reported. Many commercial companies may want to see an early end to an episode - so they get rid of the person concerned, with the exception of a number of companies who may want to make an example of the suspected fraudster. Another danger is that human nature is to avoid problems and so some people may not want to know the full extent of a problem. So, some frauds may not be investigated too thoroughly for fear of what might be found.

Levi (1987, pp.131-136) reported the views of senior corporate executives about "the *practice* of fraud reporting". It appeared that "companies with an American connection had a much tougher line on the reporting of fraud than did the British companies" (p.131). A reluctance to report fraud "often reflected uncertainty as to the consequences of reporting it – they [the senior executives] did not want to be sued for defamation – as well as a lack of confidence in the police and the Department of Trade and Industry" (p.132). One executive in Levi's study "referred to calling in the police as 'opening Pandora's box' because once they are in an organization, 'there is no telling where they will end up and what they will uncover'" (p.132). Though "to discourage re-offending and for both

retributive and general deterrent purposes was an important part of the reasons given by some executives for reporting frauds” (p.134).

Neville Russell (1998, p.5) found that only a fifth of finance directors would report an incident of suspected fraud to the police or other authority as a matter of policy. Some of the respondents said they would report the matter for the sake of having it investigated, because they had suffered significant loss or as a deterrent to potential fraudsters. The survey also found that the main identifiable reason for not reporting a fraud to the authorities was concern that it would become public knowledge. Other reasons included “a perceived lack of police interest, an inability to identify a particular individual as the fraudster and a decision that the small scale of the fraud did not justify the management time and disruption to the business that would be caused by an investigation” (p.6).

There may also be a concern that the increased reporting of fraud may lead to more copy-cat crimes. However, if the key tackling fraud is the sharing of incidents within and between companies, then it is important to learn from what has occurred.

The issue of protecting a business from fraud is very much linked to corporate governance. Corporate governance came to the fore in the 1990s and this was partly due to a number of spectacular corporate collapses brought about by fraudulent activities. The Cadbury Report (1992, p.27) points out that the directors are responsible under s.221 of the Companies Act 1985 for maintaining adequate accounting records and in order to do this they need to maintain a system of internal control over the financial management of the company, including those procedures designed to minimise the risk of fraud. There was a concern about the non-reporting of fraud and consequently there was a suggestion that external auditors should have a duty to report fraud to the appropriate authorities. The Committee did not recommend that a statutory duty to report fraud should be extended beyond the regulated sector, however, it did see scope for extending to the auditors of all companies the statutory provisions applying to auditors in the regulated sector which enable them to report reasonable suspicion of fraud freely to the appropriate investigatory authorities. Therefore, the directors have the responsibility for establishing a system of controls. If directors are not taking action to protect their companies from

the threat of cybercrime then this could be construed as potential negligence. Whilst large organizations may have the resources necessary to deal with these new threats, this is unlikely to be the case with smaller ones.

The rise of cybercrime

Over the past decade a whole new range of security threats and frauds have developed. Just to be aware of current threats and weaknesses is no longer good enough - in the words of Albert Einstein: "Imagination is more important than knowledge" (quoted by Collins, 1998, p.189). Cybercrime has been defined as:

"..a crime in which an IT network is directly and significantly instrumental in the commission of the crime. Interconnectivity is the essential characteristic; these are crimes perpetrated on and across 'cyberspace', on the information highways." (John Abbott [Director General of the National Criminal Intelligence Service] cited by Beard [2001, p.7])

Recent surveys have aimed at trying to show how the threat of cybercrime has developed (CSI/FBI, 2002) and where the current dangers seem to be (FAP/CBI, 2001; PricewaterhouseCoopers & DTI, 2002). The dangers posed by cybercrime could be summarized as follows:

"They can rob you blind. They can steal your identity. They can swipe your deepest secrets and sell them to the competition. They can read your e-mail, talk to your vendors, contact your customers, replicate your website, take orders for your products. They can avail themselves of your corporate credit cards. They can tap your treasury. They can clog your system to the point of paralysis. They can sniff through your personnel files. If they run off with your laptop, they might extort you till you weep. They might be 13 years old." (Cheney, 1999, p.38)

It is important to note that "[c]ybercrime isn't just about obtaining goods on-line using a stolen credit card, it can manifest itself in theft of information or disruption caused by hackers" (The Fraud Advisory Panel, 2002, p.1) and "increasingly sophisticated tools are available to attackers with lower levels of expertise" (Beard, 2001, p.8) - having moved from guessing passwords to www attacks and the use of advanced scanning techniques. There must be a concern that many businesses (especially smaller ones [British Chambers of Commerce, 2002]) may not have kept up with these threats. The types of problems faced include:

- web sabotage – defacement of a website is the alteration of a web

site which may be carried out to cause embarrassment to an organization, the replication of a website may be to defraud an organization:

“A recent example of web sabotage involved the Red Cross website. The Red Cross web site was cloned by hackers following the events of September 11th and for 36 hours, all donations made to the Red Cross were diverted to a cyber fraudster.” (The Fraud Advisory Panel, 2002, p.3)

- denial of service attacks – “An attack specifically designed to prevent the normal functioning of a system and thereby to prevent lawful access to the system by authorized users. Hackers can cause denial of service attacks by destroying or modifying data or by overloading the system’s servers until service to authorized users is delayed or prevented” (McAfee, 2002, p.4).
- viruses – “A computer program file capable of attaching to disks or other files and replicating itself repeatedly, typically without user knowledge or permission. Some viruses attach to files so when the infected file executes, the virus also executes... Some viruses display symptoms, and some viruses damage files and computer systems, but neither symptoms nor damage is essential in the definition of a virus; a non-damaging virus is still a virus” (McAfee, 2002, p.11). Some high profile viruses have included: “I Love You”, and “Melissa” - however, the last thing a fraudster usually wants is a high profile!
- worms – “Worms are parasitic computer programs that replicate, but unlike viruses, do not infect other computer program files. Worms can create copies in the same computer, or can send copies to other computers via a network” (McAfee, 2002, p.11). “Whereas a virus in some sense ‘attaches’ to a legitimate program, a worm copies itself across networks and/or systems without attachment. It can be said that the worm infects the environment (an operating system or mail system, for instance), rather than specific infectable objects, such as files” (InformIT, 2002, p.4). The destructive impact of the Blaster and Sobig.F worms was seen in August 2003. Worms may be downloaded via a “Trojan horse”. This is “a malicious program that pretends to be a benign application; a Trojan horse

program purposefully does something the user does not expect. Trojans are not viruses since they do not replicate” (McAfee, 2002, p.10). This could be downloaded as an attachment to an e-mail but it could also be picked up by visiting a web site. Once downloaded such a program can copy and steal data, alter other programs and even make systems crash – therefore a “Trojan horse” can be as destructive as a virus.

- hacking - where someone deliberately attempts to gain access to an unauthorised part of a computer system.

The growing significance of cybercrime was highlighted in a survey conducted by PricewaterhouseCoopers & DTI (2002:3)

“The business environment has changed rapidly over the last two years... The average cost of a serious security incident was £ 30,000. Several businesses surveyed had security incidents that cost them over £ 500,000.”

This survey also stated:

“It used to be the axiom that 90% of security incidents were caused by insiders and only 10% by outsiders. ISBS 2002 confirms that the changing business environment has altered the balance of risk. Only 34% of UK businesses reported that their worst security incident was caused by an insider, whereas 66% were caused by external sources.” (PricewaterhouseCoopers & DTI, 2002:9)

The increase in the external threat was reiterated in a US survey (CSI/FBI, 2002).

One factor resulting in the increase in this threat is:

“Cyber crime does not require physical presence at the scene of the crime; it is therefore easier to commit... Partly because of the ability to launch ‘remote’ attacks the likelihood of cyber crime being detected is significantly lower than for traditional crime” (Beard, 2001, p.7).

Another problem relates to the international nature of cybercrime. A Deloitte & Touche study (1997, pp.3-4, 36) identified hurdles relating to the investigating international fraud as including:

- differences in national laws,

- difficulties arising from communication and co-operation,
- advances in technology resulting in the physical separation of the fraudster from the victim and/ or the proceeds of any crime,
- a lack of experience in dealing with such matters,
- a lack of resources, possibly as a result of the following:
- a perception of fraud as a low political priority.

Further opportunities for the increase in cybercrime may come from the growth of broadband (faster communication enabling larger quantities of data to be transferred) and the development of symbiotic networks:

“A symbiotic network operates rather like a broadcast system. Data is first carried to a broad geographical location through a traditional network then is transferred into a symbiotic network to reach its final destination. Data is then transmitted via a wireless interface that might in the future be embedded in everyday mobile electronic devices... or in fixed sites such as buildings or street lamps.”
(BT.com, 2002, p.1)

Given the increasing use of and dependence on the internet, along with the increase in the sophistication of cyber attacks, this raises the spectre of cyber terrorism (e.g. Shein, 2001; ISTS, 2002). In the wake of 9/11 all organizations (as well as individuals) are having to recognize the changing nature of terrorism. The notion of cyber terrorism may be a new phenomenon, and maybe for this reason alone, the threat needs to be taken seriously.

The problems of researching into fraud

Given the importance and the evolving nature of fraud, this would seem to be an area worthy of substantial academic research interest, especially given the desirability of integrating teaching, research and practice (Woods and Higson, 1996). Motives for undertaking research into fraud include:

- the identification of the magnitude of the problem – to help allocate resources relating to detection and prosecution. If this is the case, which figure should be recorded – all suspected fraud (dependent, of course, on the definition of fraud used), or the specimen examples which result in a prosecution, or just the charges for which a defendant has been found guilty? It can be readily appreciated that each of these

- would result in substantially different measures of fraud.
- to educate people about the problems and heighten awareness of fraud (though depending on who is doing this, it could also be seen as a public relations exercise to generate consultancy work),
 - to assist directors to fulfill their corporate governance responsibilities,
 - to facilitate with legislative developments, and
 - to help anticipate the evolution of fraud.

Due to the dynamic nature of the problem, it is not possible to simply turn to the literature and thus it raises the question of how one researches into the future.

Given the sensitive nature of fraud, it is often difficult to approach companies directly. After all, if they did not want publicity regarding an alleged fraud, they would probably be unlikely to confide in a researcher. And even if companies were willing to discuss fraud, they may not tell the whole truth - i.e. they may say what they want others to think the situation is like rather than what it is actually like. Some companies are willing to respond to surveys sent by reputable organizations – a number of these have been referred to in this paper. However, surveys

- are unlikely to be statistically valid,
- may be biased, and
- may not be accurate.

But they do give an insight into the problem and if they are conducted over a number of years may reveal a trend. Perhaps one should remember Tukey's dictum (1962, pp.13-14): "Far better an approximate answer to the right question, which is often vague, than an exact answer to the wrong question, which can always be made precise". For an academic publication, the emphasis may be on the statistical validity of the results, with a need for unbiased and accurate data. The usefulness of academic journals as a means of disseminating results may be undermined because of the delay in publication and the limited readership.

The technical nature of the problem may limit investigation – but just because something is difficult, it does not mean that it should not be addressed. At the moment it is difficult to distinguish between "urban legends" and reality in the world of cybercrime – this alone should be enough to stimulate further research.

Conclusion

As the word “fraud” is not defined in English law, this presents a difficulty as to what exactly is meant. The dividing line between sharp practice and fraud, in certain circumstances, may at least be very fine. In a legalistic sense, a “fraud” is not deemed to have occurred until it has been proved in court (after all, at first sight something may appear to be a fraud, but on investigation this may not be the case). Therefore, the mere reporting of suspected frauds discovered is unlikely to indicate the true magnitude of these crimes.

Generally, the treatment of a suspected fraud is at the discretion of the directors (though external auditors do have a “public interest” duty). As part of their corporate governance responsibilities, consideration could be given to requiring directors to ensure that suspected “frauds” are thoroughly investigated internally. The creation of a company policy document regarding the treatment of a suspected fraud may help clarify the directors’ responsibilities.

In a previous study (Higson, 1999), one of the participants posed the question: “What does a fraudster need?” His answer to his own question was:

- honesty and trust (to take advantage of),
- naivety, and
- organisational change (e.g. downsizing - possibly resulting in a loss of knowledge and experience).

The advent of the internet and developments in e-commerce have certainly increased the level of “naivety” regarding the threats that they create. The dangers from cybercrime, cyber fraud and cyber terrorism are relatively new phenomena and the real danger is that companies may only learn about them very slowly – as they suffer the consequences.

References

Auditing Practices Board (APB) (1995), “Fraud and Error”, Statement of Auditing Standards 110 (issued January 1995), in *Auditing Standards and*

- Guidance for Members*, London: ICAEW, 2002.
- Beard, A. (2001) "Cyber crime – a growing concern for e-business", *Corporate Governance*, March: 6-9.
- British Chambers of Commerce (2002) *Using IT: Small Firms and Technology Survey Report*. London: British Chambers of Commerce.
- BT.com (2002) *Anytime, anywhere and anyhow*
http://www.catalist.bt.com/white/anytime_01.html (viewed on 04/10/2002)
- Burns, S. (1998) "Easy Money", *Accountancy*, August: 38.
- Cadbury Report, The*, (1992) Committee on the Financial Aspects of Corporate Governance. London: Gee.
- Cheney, G. (1999) "Cyberfraud and Computer Crime: What the CFO needs to know", *Strategic Finance*, November: 38, 40-43.
- Collins (1998) *Collins Concise Dictionary: Quotations*. Glasgow: HarperCollins Publishers.
- Comer, M.J.(1985) *Corporate Fraud*. Aldershot: Gower.
- Computer Security Institute/ Federal Bureau of Investigation (CSI/FBI) (2002) *2002 Computer Crime and Security Survey*. San Francisco: Computer Security Institute.
- Davies, D. (2000) *Fraud Watch*, 2nd edition. London: ABG Professional Services.
- Deal, T.E. & Kennedy, A.A. (1982) *Corporate Cultures*. London: Penguin.
- Deloitte & Touche (1997) *Fraud without frontiers*. [London]: Deloitte Touche Tohmatsu International.
- Elliott, D.J. (2000) *Preventing Fraud and Corruption in the Public Sector: Changing Managerial Cultures*, unpublished M.A. Thesis, Liverpool John Moores University.
- Ernst & Young (2000a) *Fraud: Risk and Prevention*. London: Caspian Publishing Ltd.
- Ernst & Young (2000b) *Fraud The Unmanaged Risk: An international survey of the effect of fraud on business*. London: Ernst & Young.
- French, D. (1985) *Dictionary of Accounting Terms*. London: ICAEW.
- Fraud Advisory Panel (2002) *Cybercrime – what every SME should know*. London: The Fraud Advisory Panel.
- Fraud Advisory Panel/ Confederation of British Industry (FAP/CBI) (2001) *Cybercrime Survey 2001*. London: CBI.
- Higson, A. (1999) *Why is management reticent to report fraud? An exploratory*

- study*. London: The Fraud Advisory Panel.
- Higson, A. (2002a) *Indications of Fraud in SMEs*. London: The Fraud Advisory Panel.
- Higson, A. (2002b) A review of “*Forensic Accounting*”, *British Accounting Review* December, pp.419-422.
- Huntington, I. and Davies, D. (1994) *Fraud Watch: A guide for business*. London: ICAEW.
- InformIT (2002) *Viruses and Worms*, InformIT.com.
- Institute for Security Technology Studies (ISTS) (2002) *Cyber Terrorism: The State of U.S. Preparedness*.
<http://www.ists.dartmouth.edu/ISTS/counterterrorism/preparedness.htm>
- Levi, M. (1987) *Regulating Fraud: White-collar crime and the criminal process*. London: Tavistock Publications.
- McAfee Security (2002) *Virus Glossary of Terms*. http://www.mcafee.com/anti-virus/virus_glossary.asp
- Neville Russell (1998) *Dealing with fraud: A survey of UK companies*. London: Neville Russell, February.
- Oakes, R. and Standish, P. (1996) *Organisational Values as Contingent Variables in Fraud*, presented at the British Accounting Association National Conference, Cardiff Business School, March.
- PricewaterhouseCoopers & DTI (2002) *Information Security Breaches Survey 2002*. London: PricewaterhouseCoopers & DTI. <http://www.security-survey.gov.uk>
- Shein, E. (2001) “Are companies prepared for Cyber-Terrorism?” CFO Magazine. <http://www.cfo.com/article/1,5309,5900,00.html?f=related>
- Tukey, J.W. (1962) “The Future of Data Analysis”, *Annals of Mathematical Statistics*, 33.
- Woods, M. and Higson, A. (1996) “The interface of accounting research with education and practice”, *Accounting Education*, 5(1), pp.35-42.