The Fraud Advisory Panel

the fraud advisory panel

Indications of Fraud in SME's

Indications of Fraud in SMEs

Dr Andrew Higson
Loughborough University Business School

Executive Summary

Small and Medium-sized Enterprises (SMEs) make up the majority of businesses in the UK. As the type and nature of the frauds they face are likely to be different from those faced by larger entities, this study was aimed at identifying these threats and the indications that such frauds may be occurring. Whilst many of the frauds discovered in this sector may be committed by owner-managers, this study focused on the frauds by employees and third parties against such businesses.

In an SME, there may be fewer internal controls, but managers may be more in touch with what is happening than in a larger organisation. Trust is something that smaller enterprises may have to depend on, but it is something that could easily be abused. Therefore, it is important that there are adequate personnel checks when recruiting new employees. The culture which exists in an organisation is an important factor in its vulnerability to the threat of fraud. Managers need to give a clear lead and set the standard of acceptable behaviour.

The most prevalent types of fraud are likely to be those that impact on the profit and loss account as a result of the overstatement of expenses or the understatement of income. These may not necessarily be large and so they may be difficult to identify.

A time when an SME is particularly vulnerable to fraud is during a period of rapid expansion. The dynamics of the situation may mean that it is more difficult for managers to have an overview of the business.

Advances in technological developments mean that all organisations that are connected to the internet are vulnerable to attack from outside. Whilst larger organisations may have the technical knowledge to minimise this threat, SMEs may not even recognise the risks.

Whilst SMEs may not be able to have as many internal controls as larger organisations, it is imperative that their managers evaluate the risks that their businesses face and ensure that they at least have defences in their key areas.

Introduction

Small and medium-sized business entities (SMEs) are the most prevalent type of business in the UK. As a rule of thumb, an SME is usually regarded as an organisation comprising fewer than 250 people. Even within this range, it must be appreciated that the problems faced by a very small organisation (with only a handful of employees) may be very different from the problems faced by an organisation at the top of this range. A survey by the ACCA (2001:8) indicated that: 75% of frauds in smaller businesses were committed by owner-managers themselves; 20% were

committed by employees; 2% were committed by owner-managers colluding with employees; and a further 1% were committed by employees colluding with third parties. The aim of this study was to concentrate on examining the threat of fraud against SMEs, and therefore was not looking at frauds committed by owner/managers, however, it did cover frauds committed by senior employees against the business.

Bearing in mind the definitional problems relating to fraud as well as the "uncertainties" as to whether something is or is not a fraud (e.g. Higson, 1999), the objective of the study was to obtain opinions about the problems faced by SMEs in relation to the threat of fraud. This study was funded by the Fraud Advisory Panel. Sixteen interviews were conducted with a variety of organisations (see the appendix). The study also reports cases based on the author's own experiences. No comments have been attributed to individuals, organisations or clients.

The threat of fraud

It is all too easy to think of fraud as someone else's problem. When people set up their own businesses, the threat of fraud may not be a major concern - its importance may only gradually dawn on them. Managers may tend to be more worried about the bank manager, the tax inspector and the auditor than the threat of fraud. However, in recent years there has been a tendency for fewer external professionals to be involved with the running of these businesses. For example, in the past an SME may have had more contact with the bank, the VAT investigators may have carried out more checks and the business could have been subjected to an external audit. Therefore, in the battle against fraud, managers may be becoming more isolated.

The threat of fraud has always existed, however, the opportunities for it may now be expanding:

- An increasingly educated workforce may be able to overcome a company's internal controls. In the interviews it was suggested that there may be fewer moral checks these days and thus people could be more willing to take risks. In particular, it is always necessary to be on the look-out for the disaffected employee.

A person set up the IT system and adjusted it to pay himself an extra salary (randomly within a certain range). This was only discovered by a consultant after there had been suspicions about someone else. The consultant spotted the rogue subroutine and it was traced back. The person left the organisation, however, there was another subroutine containing a "Trojan horse" virus so that when this person's name was removed from the system, it wiped out the accounting system.

- Desk-top publishing means that it is easier to produce dummy invoices, bank statements and other third party documents - hence the importance of the control function.

- Many organisations are increasingly outsourcing key functions. These may include:

The IT function. This can be a major concern especially as systems are becoming more powerful and many people do not fully understand them. There is a view that the computer must be right and therefore fewer manual checks may be conducted.

The increase in the inter-connectivity of businesses means that more people have access to the business (electronically). Physical access was the key in the past, but now it is possible to give away the electronic keys to an organisation's systems.

The accounting function. Smaller businesses may not have a full-time accountant and they may be unwilling to pay for an external accountant to prepare monthly or quarterly figures. This means there is often a delay in obtaining the financial figures - thus providing a window of opportunity for a fraudster.

It is important to have systems that produce reliable figures, however senior managers often lack knowledge of their own systems. In one example that was cited, the management did not know the Sage password for the accounting system, and consequently they were not looking at the accounting figures because they were unable to access the system. Management was totally dependant on someone from outside the business to update the figures every two weeks. If management did not have access to their own system, they could not know what was happening. This can be a major problem if a business is growing rapidly. A business may start off well, but if management do not have up-to-date figures (and if there is not a budget to compare against), then there is a danger of over-trading (i.e. whereby a business grows too rapidly and thus over-stretches itself).

If SMEs do not have budgets it is difficult to monitor the financial figures on a regular basis. Managers may have a natural instinct about what is happening, and the financial statements may then be used to confirm these feelings. However, if something has gone wrong, the time lag in producing the figures (especially if it is only done on an annual basis), may mean that it is too late.

Other professional services. For example, SMEs may hire consultants - it is important that these people are competent, that the terms of reference are set out and that the work is performed to a professional standard.

Contract tendering (kickbacks). Tendering may be seen as a way to obtain best value from a contract, however, if the process is corrupted by bribes and sweeteners, it may actually result in inefficiencies and dubious quality.

So, whilst it may make sense to outsource some activities in order to enable management to maintain its focus on the key aspects of the business, it can also produce additional risks.

- There may be a greater risk if a business is rapidly expanding. The directors may be good at the core activities but then they have to depend on others for the accounting support, the human resource management and keeping abreast of IT systems developments.

- Organisations may be more prone to cost-cutting than in the past, but is the cost/benefit always analysed? This may result in fewer people in management with fewer checks - this may be a particular problem for organisations at the top end of the SME range.
- Whilst there is no evidence of any current problems, the development of stakeholder pensions may present a potential threat in the future. There is a tendency for change to equal risk, therefore, attention needs to be paid to the new payroll procedures and the transfer of funds to the pension providers.

Generally fraud may be divided into two main types:

Profit and loss frauds (e.g. understating revenue or overstating expenses): SMEs are likely to be vulnerable to a variety of small frauds. These may be difficult to detect as individually they may be for relatively small amounts (though over time they may be significant). Large frauds would be likely to be discovered (whether this is in time to save the business is problematic). Therefore, in terms of impact, the amount of time taken to spot a fraud is key.

Balance sheet frauds (e.g. cut-off problems, accounting data manipulation, etc.): These often tend to increase in size – thus leading to discovery. However, the ACCA survey (2001:3) stated "that fraud within smaller companies does not involve fraudulent financial statements" (i.e. misstated financial reports), but this may not always be the case. One interviewee reported the following example:

A finance director created fictitious sales and assets (debtors) near the year-end in order to show that the business was profitable. This was to ensure that the bank would continue its support. In the short-term it was possible for him to justify to the other directors why the debtors had not yet paid, but as time went by they became suspicious. This was reported to the police but by that time the finance director had left the country in order to escape prosecution.

Trust may be more crucial in an SME than in a large organisation. As an SME is unlikely to be able to afford a comprehensive system of internal controls, trust then becomes an important factor. A person may have the inspiration to create a business but it is unlikely that he/she will also have the accounting skills, IT skills, knowledge of the regulatory framework, etc., necessary to run the business. Trust has to exist in a small management team - but it is also something that is easily abused.

Some businesses may simply live with fraud as a fact of life, but this does not mean they should not take action to minimise its potential impact. If a business makes a profit of 20% on its sales, then a fraud of £100 a week (approximately £5,000 a year) will result in it having to generate an extra £25,000 in turnover to make up the deficit. So, whilst some businesses may live with fraud, it is not an easy life.

Types of fraud faced by SMEs

The susceptibility of an organisation to the threat of fraud probably depends on its type of business - products that are easy to dispose of tend to be more susceptible to fraud. Whilst the risk of fraud may be greatest in those businesses handling cash or attractive consumer goods, it must be remembered that all businesses are vulnerable to fraud of one sort or another.

The danger from fraud may come from three broad categories:

1) Employees abusing their position:

The misappropriation of assets (such as cash, stock, reimbursement of expenses, payroll, stationery, etc) - these tricks are as old as time.

In a builders merchant business, an employee in the yard was taking back-handers for overloading delivery vehicles. The lack of a division of duties meant that one person was doing everything. Due to the nature of the merchandise it was difficult to spot what was happening. The scam showed up once another employee becomes suspicious – this person was looking for a specific item of stock but it had gone. Once suspicions had been aroused, management started to watch the employee and more checks were conducted. Eventually there was enough evidence and the person was dismissed. The level of fraud was such that it was considered to be not worthwhile taking further action. The duration of the fraud was never discovered.

Employees' usage of the telephone for personal calls would be another example of the misappropriation of an organisation's assets. A recent development is the abuse of internet access - not only can this be a waste of staff time, it may incur call charges, but more seriously it may lay the organisation open to attack from computer viruses and hackers.

The manipulation of documents - this can include altering documents as well as producing false ones.

In a timber yard, the gate man was in league with a delivery driver. Items would be loaded onto the delivery truck but then crossed out on the despatch notes. Over time, suspicions were aroused by the number of alterations to the delivery documents. Consequently an investigation took place and the fraud was uncovered. Because of the drip feed nature of the fraud it did not show up in the gross margin percentage.

Theft of confidential information (e.g. client/customer lists) or of intellectual property (e.g. a manufacturing process) - the building up of a client list is very time consuming and so there is always a danger that when a senior person leaves, they may take the information with them.

Bonus-based frauds – managers may manipulate information on which their bonuses are based (performance bonuses are now relatively common in management packages). Whilst performance bonuses may motivate some people, they can also lead to dysfunctional behaviour. The recording of sales may be delayed if the person has already achieved their target figure, or sales may be "anticipated" in order to hit the target. If someone consistently underachieves their target, then this type of fraud may start to be displayed (n.b. as it is now more common for people to change jobs relatively frequently and this may only be discovered after they have left).

"Teeming and lading" (whereby cash may be misappropriated by falsifying the accounting records) may not be as prevalent as in the past. This may be because computerisation has made it more difficult.

Employees taking unwarranted sick leave could be classified as a fraud. However, this sort of thing would not be reported to outside authorities. The onus would be on management to monitor and deal with the situation.

The gullibility of employees - if something is too good to be true, then it probably is:

A half million pounds was paid into the Jersey bank account of someone who had promised to double the money for the company in a month – the mechanics of doubling the money were not explained! Although two people had to sign the bank transfer, one had been hoodwinked and the other person just signed. At the end of the month the money was not returned: "There was a bit of a problem". After waiting five months the auditor was contacted. Following a forensic investigation the police were also informed. By this time there was no money left in the Jersey bank account - it had long gone.

Signing blank cheques - many businesses require two authorised people to sign cheques. When signing it is important to check back to the supporting documentation to ensure that the payment is valid. There is a danger that people may sign cheques in advance because of the "hassle" of signing them individually. This would be a major control weakness, yet it does happen. Not only does this mean that the check which should have been there, is not, but also it was easier to misappropriate cheques.

2) Suppliers may take advantage of their customers:

A supplier of goods may recognise weak or non-existent checking controls. This can result in fewer items being delivered than stated on the delivery note, or even the wrong type of goods. Without sufficient checks on goods received it may be difficult to complain later. Another trick is to invoice for the wrong quantity or at the wrong price. To overcome this it is important to check back to the original order and the delivery note (assuming that this was checked when the goods were delivered).

The company purchaser may not be independent (e.g. he/she may be related to, or be taking back-handers from the supplier). This can result in substandard goods being bought at an uncompetitive price.

Directory fraud is whereby a letter and invoice is received thanking the company for agreeing to an entry in a directory. Unless the business has an authorisation process to weed out fictitious invoices, there is a danger that the recipient will pay simply because their company's name is on the invoice.

Failure to collect debts may indicate fraudulent activity - e.g. fictitious sales or misappropriated receipts.

Franchise frauds – fees may be taken, but the supplier may not provide a proper service.

Unauthorised insurance – a person/business claims to be an insurer when they are not they may infer that they are part of a reputable company. A recent example was selling insurance to mini-cab drivers in London. This could result in the drivers themselves committing an offence.

When considering supplier fraud it is often difficult to distinguish between it and sharp business practice (Burns, 1998).

3) Whilst businesses need their customers, it may be better to do without some of them:

During the expansion of the business, it may be necessary to take risks on customers without due diligence (i.e. proper checks). These days businesses are almost forced to accept credit cards. Credit card fraud can include:

"card not present" frauds (e.g. over the telephone, internet etc.). The retailer may carry out little background checking (e.g. may not correlate the address and delivery address). With this sort of fraud the retailer bears the loss.

"card present" frauds (e.g. someone presents a stolen, or forged card in person). Providing that the retailer has conducted all the checks that the credit card company requires, then the credit card company bears the loss. The retailer can still make things difficult for a potential fraudster (e.g. asking for more proof of identity), but it often depends on how desperately the sale is required.

Product theft/bad credit (long firm fraud) - some businesses may be specifically set up with the aim of obtaining credit facilities and then obtaining goods without paying for them. British industry may live on credit, but it is important to be careful about the customers to whom these facilities are granted. Numerous businesses are forced into liquidation because of the non-payment of a debt by a customer.

More significant frauds may occur if employees collude with either suppliers or customers.

Another possible source of threat may now come from the internet. Programs such a "Trojan horse" may be downloaded when using the internet (this may come in the form of an attachment to an e-mail, but it could also be picked up by simply visiting a site). Once downloaded such a program can copy and steal data, alter other programs and even make the system crash. It is important to have "fire walls" in place in order to protect systems and data.

Another threat to an organisation's security can come about when upgrading or replacing a computer system. Data may still remain on the system (e.g. temporary files, or files that have not be fully deleted) and so an unscrupulous computer consultant/retailer would be able to access what were confidential files.

So, whilst many types of fraud are as old as time, technological developments may present a whole new range of threats to SMEs.

Are there factors specific to SMEs that may make them vulnerable to fraud?

Managers may be experts at what they do but may be less skilled in business. Some people are driven to setting up their own business because of their experiences in larger businesses. As a consequence they do not want to mirror those experiences, therefore there may be greater trust (e.g. no time sheets etc). In smaller businesses trust is very important. In an SME the level of trust utilised may go beyond the normal employer-employee relationship (substandard performances may be tolerated because of loyalty), and people are often unwilling to contemplate the idea that someone is defrauding them. Managers may not perceive the risk and may be too trusting (especially in terms of business partners or long-serving employees).

SMEs per se may not necessarily be more vulnerable to frauds than larger organisations. There was a view that in a small company people may feel they have a greater stake in the business, so this could mean they are less of a threat to the business. Senior people may be more in touch with the business, and thus have a good "instinct" or "feel" about what is happening. Indeed, as an organisation grows it may actually become more inefficient. Therefore, smaller organisations may be less bureaucratic, and a greater working knowledge of the whole organisation may mean that managers are more likely to spot and question unusual things. If a small number of people are involved with the control system, it may be more difficult to hide things from such a team.

Having said the above, as an organisation grows, a coherent system of internal controls becomes a necessity. The internal control system "comprises the control environment and control procedures. It includes all the policies and procedures (internal controls) adopted by the directors and management of an entity to assist in achieving their objective of ensuring, as far as practicable, the orderly and efficient conduct of its business, including adherence to internal policies, the safeguarding of assets, the prevention and detection of fraud and error, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information" (APB, 1995: SAS 300: para.8).

Examples of internal controls:	Orientation
Plan of organisation	Internal
Segregation of duties - may not be practical	Internal
Supervision	Internal
Arithmetical and accounting	
- accounting knowledge	Internal
- budgeting and comparisons	Internal
Authorisation and approval	Internal/External
Physical controls	Internal
Personnel controls	Internal
Management controls - business knowledge	Internal/External

Because of the higher level of trust, the control environment in an SME is often less defined therefore there may be more scope for fraudulent activity.

An important tool in controlling a business is the accounting system, however, many managers may have a poor knowledge of accounting. The lack of this technical ability, may mean that people may not recognise what they are seeing, even if there are signs that everything is not alright. Smaller business may not employ budgeting, may not split margins by products, and may only check stock once or twice a year. Regular checks are important, e.g. stock checks, bank reconciliations, and checking creditor statements. The management accounts may not have any resemblance to the financial accounts (accruals and cut-off may not be done diligently in the management accounts), and consequently, there is a danger that as a tool they may not have credibility with the entrepreneur.

It is often thought that smaller organisations cannot afford to put a comprehensive set of controls in place. Segregate duties may not be practicable because of a lack of staff and because the perceived cost/benefit may not be there. Authorisation, accounting, and physical controls may be high in terms of priority, but personnel controls are often perceived as being of low priority. Many SMEs do not really have a human resource (HR) function - yet the choice of an employee is crucial in the battle against fraud. Often there is no time or inclination for pre-employment screening and many may not take up references. There may even be fewer due diligence checks with the appointment of a senior person than a junior person. Often it is the reputation of the previous employer that counts – and it is not considered that this employer may be only too happy to be rid of them. Sometimes it is difficult to read into what is being stated in a reference, and employers are often reticent to be explicit in a reference. Getting good people, especially on low wages, is not easy, and so the lack of formal employment procedures may result in the employment of dishonest people.

Even if due diligence checks are carried out when someone is employed, it is important to remember that an individual's circumstances may change over time. Personal troubles or pressures may turn what was an honest employee into a dishonest one - this potential threat is often overlooked.

Another problem is that there may be little development of employees with a lack of training and career structure. It may not be easy to motivate these employees. Whilst some employees may be happy with this, others may become resentful or bored - a disgruntled employee presents a greater risk to the business.

Therefore, three things can be said to be critical in understanding why frauds occur:

- there are no controls (so there is plenty of opportunity);
- the controls that are in place are not implemented properly; and
- generally there is a lack of supervision (people are too busy to do things and they get left).

In the battle against fraud there needs to be attention to detail. It is the things done before the event (to prevent it) that are as equally important as what to do after the event.

The impact of frauds on an organisation

Obviously, the impact of a fraud depends on its nature and size. Frauds in SMEs are seldom widespread enough to sink the business, but they may mean that they make it more difficult for the business to grow if it is being drained of resources. A fraud may also reduce the ability of a business to survive in harsh economic conditions. If a business is operating from hand-to-mouth, it is unlikely to have "spare" cash, and so will not be cushioned from the effect of a fraud - this may make them particularly vulnerable. Therefore, potentially even "small" frauds could bring down a business. Although this may be rare, it is important to remember that the owner/manager could be personally liable for the debts of the business if he/she has given guarantees in respect of any loans or overdrafts. The full impact of a fraud may be mitigated by fidelity insurance - if this exists.

A fraud may be committed because the business is failing. An individual may take action to try and tide over the business until things pick-up. However, the fraud may get larger and larger if the turn-around does not come - therefore, this type of fraud may only be detected when the business collapses and may even be a contributory factor to the collapse. If senior management is being given misleading information, they may not realise the full extent of the problem and may take the wrong decisions.

The discovery of a fraud may be more significant in terms of breach of trust rather than the amount per se. It can create an atmosphere of distrust within the organisation. Any scandal can also have a serious impact on an organisation's reputation. Therefore, whilst an organisation may claim that it cannot afford internal controls, it may not be able to afford not to have them.

The impact of culture on an SME's vulnerability to fraud

There was strong support for the idea that culture is everything when it comes to combating the threat of fraud. It is important that people are given guidelines – and for an example to be set. Elliott (2000:30) considered:

> "The simplest definition of culture is 'the way we do things around here' (Deal & Kennedy, 1982). Although this is a very straightforward definition, in practice culture is very difficult to specify, isolate, understand and alter."

As a consequence:

> "The starting point has to be with the organisation itself conveying a clear message to staff that dishonesty in any form is unacceptable and that action will be take against any transgressor regardless of their position. This message must be backed up and supported by the actions and principles of senior management.
>
> "Failure to follow the principles and failure to take action to which management is committed is an act of moral weakness and will undermine the credibility of management. As per Johnson's [1992] cultural web this will become one of the myths and stories on which the real culture of the organisation is founded. In summary, don't make a promise you can't keep or a threat you don't intend to carry out." (Elliott, 2000:33-34)

Therefore, the style of management will create the environment in which employees operate. A management style that is too domineering or too weak will each create its own problems. The personality of the person leading the organisation is important and their involvement in running the business is the key. However, if owners do not make a distinction between personal assets and corporate assets, it is unlikely that the employees would act differently. If the workforce sees that the directors have their own unethical codes of business behaviour, it is soon going to permeate down the organisation. If the managing director lives off round sum expense allowances this is bound to have an impact on others: 'Monkey see, monkey do'. Whereas, if a business has a culture of honesty and ethical behaviour, the chances are that any fraud will be discovered because others will not let it happen.

How are frauds discovered?

One person expressed the view that the vast majority of small frauds were probably not discovered. Elliott (2000:33) 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."

As a fraud develops, it is likely to become more complex and therefore the perpetrator has more and more to remember. As a result, errors are more likely to occur and thus the fraudster may be unmasked:

An accounts clerk had the responsibility for reimbursing expenses through the payroll system. Sales reps would submit their travel expenses to this individual and he would arrange for payment to be made by a direct transfer into their bank accounts. The clerk was able to change the bank accounts as necessary. This person started producing bogus claims in the names of the sales people which were then approved in the normal way, but when the payment was due to be made, the bank account details were changed to that of the clerk's bank. The fraud was discovered when a sales rep's bank account was credited with money for which no claim had been made. As the clerk was not in the office when the query came in, someone else investigated it and discovered what had been happening. On this item the clerk had forgotten to change the bank details to those of his own account. The clerk was confronted and admitted to falsifying claims for £8,000-£9,000 which he offered to pay back. The clerk was suspended and not allowed further access to the records. After a full investigation, it was reported to the police and he was prosecuted for theft – over four years the fraud had amounted to approximately £100,000.

A change in routine can also help to bring frauds to light. This could be while someone is on holiday or on sick leave. Thus a fraudster may take little holiday or have very good health. Frauds can also some to light after the fraudsters death. More often than not, frauds are discovered totally by chance:

In the back office of a DIY shop a little old lady was responsible for recording the petty cash. Following her sudden death, the accountant had to take over her job. On writing up the petty cash book he found that some £400 was missing. In order to protect her good name (as she could not defend herself) he decided to make up some expenses in order to off-set the missing money. When the auditors arrived they found that the accountant had inadvertently recorded one week's cash takings twice in the petty cash book and thus had overstated cash by £400. When approached by the auditors he explained that he made the mistake in the chaos following the petty cashier's death and he explained to them what he had done. The auditors then asked him to identify the false expenses – the only problem was that the accountant could not identify these items because over the years he had had so much experience at making up expenses and so he had become very good at covering his tracks. So even though the fraudster knew how much he was looking for and the time period in which this incident had occurred, even he was unable to identify his own false expenses. The accountant left the business soon after this.

An indication of a fraud could come from outside of the organisation. For example, the bank may question the payee's name on a cheque. This may have been altered prior to despatch or intercepted in the post. A customer may complain about the goods they have received. These complaints should be recorded and monitored as they may indicate that there is a problem in the despatch area. It is always important to be on guard against "accidents" as this may just be an excuse to cover up something. If suspicions are aroused it is important that the matter is investigated.

A fraud may come to light after an anonymous tip-off maybe via letter or an especially created telephone hotline for whistle-blowing. It is always important to be on guard against malicious intent in such a tip-off, however, it could be that someone may be jealous because they can't have a share in a scam, or there has been a break-down in a relationship and someone wishes "to get even".

Occasionally, the fraud may come to light because it has become so large that it cannot be hidden any more - but this sort of situation is probably exceptional. It is rare for external auditors to discover frauds - they plan their work to have a reasonable expectation of detecting material errors and omissions. This is because many frauds encountered in SMEs are likely to be small relative to the whole organisation.

Frauds may be discovered on the winding up of a company - but, of course, by this time it is too late!

Indications of fraud

The signs may be there, but whether people see them is a different matter. Therefore, the danger signals may go unnoticed. Often it is only with the benefit of hindsight that something may be apparent. Some indicators may be:

- Variations in accounting ratios (e.g. gross profit margin, net profit margin, debtor days, creditor days, etc.). If managers are not familiar with these terms, they probably do not know if a fraud is being committed in their organisation!

The managing director of a timber merchant was concerned when the gross margin for his business fell from 25% to 23.5%. This may not seem like much of a change, but he thought it was significant and he could not think of any factors to account for it. He investigated the situation, but could not find anything and so he informed his auditors. The auditors investigated, they could not find anything either. Then, by chance, an employee was passing the timber yard one weekend, when it was supposed to be closed. This person noticed that a lorry was being loaded with timber and this was reported to the management who brought in the police. What had happened was that an employee had obtained a copy of the key to the gate of the timber yard and was going there at weekends with some accomplices to help themselves to the timber which they subsequently sold on to the building trade. Because of the lack of internal controls over the stock, bundles of timber could go missing without really being noticed - it was only the accounting numbers that were highlighting the existence of a problem.

- A change in the cash flow - but for this to be noticed, it requires monitoring. When the bank calls, it is often too late.
- Stock out, stock shrinkage or poor quality stock, may be indications of a problem.
- Customer complaints - informal contacts with suppliers and customers may give a different perspective.
- Employees' lifestyles/drug addictions may indicate potential problems. Changes in lifestyle would be very unusual and would involve a large amount of money which would probably be noticed.
- Lack of holidays, this may be a sign of enthusiasm, but it may also be to cover up something.
- High turnover of staff may indicate a problem (or just a bad management style).
- Although enquiries about something unusual may be made, people tend to be trusting, and so they may be fobbed-off.
- A computer virus/computer breakdown may be a symptom of something more sinister (e.g. an attempt to hide a fraud).

Further warning signs can be found in Ernst & Young (2000a). Whilst "red flags" may be useful in some businesses, often SMEs (because of their size and lack of internal controls) may not give these signals - or at least, not until it is too late.

Actions taken when a fraud is suspected

Managers may not know what to do when a fraud is suspected, especially if there is no contingency or formal response plan in place. If something untoward is suspected, a common response may be denial and then anger and then a desire to get even. However, the response should be measured. The circle of knowledge needs to be kept tight. It is necessary to understand what has happened – this needs to be done discretely, but damage limitation also needs to 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 take appropriate action. 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.

If a fraud is suspected, managers may deal with it internally only because they may not appreciate the difficulties involved in a proper fraud investigation - especially in obtaining and safeguarding the evidence. The options open to management include:

- Conduct an internal investigation.
- Inform the external auditors.
- Bring in external investigators/forensic accountants/security consultants (may be observe the situation with hidden cameras or through some other surveillance).
- Change the internal controls, or instigate new ones.

During the audit of a small manufacturing company, the auditors were carrying out their examination of the client's stock schedules. Total stock amounted to £72,000, however, the auditors noticed that the single largest stock item (amounting to £12,000) had been included on the stock sheets twice. As a result, stock and profits were each overstated by £12,000. When this was brought to the attention of managers they were naturally surprised and wondered how it could have happened. An adjustment was made to reduce the stock figure and thus the profit. Was this an attempt to boost profit in a lean year and thus a fraud, or was it a genuine accident? In this instance, the difference between a fraud and an accident would seem to be the motivation behind the event. What would have happened if this 'error' had been undetected and three months after the end of the audit the company had gone into liquidation? If the liquidator had spotted this in the wreckage of the business no doubt the conclusion would have been that it was a fraud.

Once enough evidence has been gathered and the perpetrator has been identified then there are a number of options open to management. This could range from a verbal reprimand, a formal warning, reimbursement, dismissal, or a report to the police. The police may have to be informed for insurance purposes, however there is a perception that the police will only investigate if the fraud is for a significant amount, e.g. over £250,000 (Higson, 1999). Even more worryingly, managers may not want to investigate because it would take up their time and thus deflect them from running the business. However, if something has gone wrong, it is important that management learn from this experience, otherwise it is likely to recur.

What could be done in order to reduce the threat of fraud?

The only real way of dealing with the threat of fraud is by putting good preventative measures in the system. However, a lot of time and money could be spent instigating a series of internal controls, but would they be cost effective? It is necessary to think about all the areas of the business that are potentially vulnerable to fraudulent activity. If this is too large an exercise to undertake, this in itself is significant! Maybe, consideration should be given to bringing in someone else.

In terms of a risk assessment, it is important to think about:

- Where does most of the revenue come from?
- Where is the most cost?

It is these areas that may more easily conceal fraudulent activity. Whilst there is much talk about the external threat of fraud, directors may not have thought about the threat from inside the organisation itself. So, after identifying the key risk areas, consequently, consideration should be given to increasing the priority of the internal controls in these areas.

- Physical security: simple steps like restricting access to parts of the organisation, implementing passwords on the computer system (and keeping them secret), keeping company documents secure, etc.
- Delivery and despatch checks: do you know what is being received and despatched?
- Daily banking of cash: this may deter staff from "borrowing" money.
- Monthly bank reconciliations: this could highlight any changes to cheques, money not being banked, unauthorised withdrawals etc.
- Future plans set out in a budget would enable a comparison to be made with the actual results. If budgets do not exist, does the business know that it will have the capacity it needs, the cash that it needs and the other resources necessary to achieve its targets?
- Implement extensive/proper credit and background checks. Be careful if the delivery address is somewhere else. Maybe employ an agent to do a private investigation.
- On the employment of an individual obtain references and examine such things as passports/N.I cards/work permits, educational certificates, etc – however, forging these documents is a major activity.
- Once someone is employed:

  - Monitor time sheets.
  - Check expenses – an ultra-violet light should detect alterations to expense vouchers.
  - Monitor sicknotes.
  - Watch out for changes in employees' behaviour.

- When someone leaves conduct an exit interview, or arrange to speak to ex-employees informally, say in the pub. Meeting up with someone (e.g. for an informal drink) after they have left the organisation may be a way of finding out what is really happening. A person may be more willing to speak freely once they have left than when they were an employee – they may have left because they did not like what that they saw.
- When someone leaves, cancel their passwords and ensure that they cannot come back on site:

A person left an organisation, but his details were left in the IT system (even his password remained unchanged), and so he was able to take revenge on the organisation and hack back into the system.

- A fraud policy statement should make it known that fraud will not be treated lightly (Fraud Advisory Panel, 2002:4).
- A fraud response plan would set out the steps that need to be taken. However, few SMEs have one, but it is better to show that you have thought about the problem than to blindly start an investigation.

It is important to follow up suspicions. Very rarely is a fraud 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.

Conclusion

The threat of fraud has always existed, but in today's dynamic and aggressive business world, the danger is probably greater than ever before. In the past more external people may have been involved with the operations of an SME. For example, the raising of the audit threshold may mean that the discipline it imposed has been lost to many companies, and one of the few sources of external scrutiny may have been denied.

Trust is an important component in the workings of an SME, but this is also something that can easily be abused. Careful consideration has to be given to the procedures to recruit new employees - because frauds are committed by people, and an organisation is very vulnerable to the threat of fraud if its employees are corrupt. It has been suggested (Higson, 1999:24) that the factors necessary for a fraud to succeed include:

- The existence of honesty and trust (in order for the fraudster to take advantage of them).
- Naivety (i.e. the lack of imagination as to what could be happening).
- Organisational change (e.g. downsizing - possibly resulting in the loss of knowledge and experience).

Perhaps the major change in the past few years has been the way in which businesses use information technology. Hardly any business has been left untouched by this development. SMEs need to recognise potential weaknesses in their own systems in order to realise how they may become vulnerable to attack (whether from inside or outside).

Inevitably, an SME cannot afford the level of internal controls that larger organisations may have, however, this does not mean that they should be totally forgotten. Managers need to be aware of the key areas in their organisation that may be vulnerable and then identify the main risks. Focusing on the prevention of fraud is probably the key to protecting an SME.

Further Reading

AAA Auditing Standards Committee (2001) 'Fraud: A Review of Academic Literature', *The Auditor's Report*, 24(2):3-5, 9.

ACCA (2001) *Members Survey: Fraud and the Smaller Company*. London: ACCA.

APB (1995) *Statement of Auditing Standards 110: Fraud and Error*. London: APB.

APB (1995) *Statement of Auditing Standards 300: Accounting and internal control systems and audit risk assessments*. London: APB.

Beasley, M.S., Carcello, J.V., Hermanson, D.R. & Lapides, P.D. (2000) 'Fraudulent Financial Reporting: Consideration of Industry Traits and Corporate Governance Mechanisms', *Accounting Horizons*, 14(4):441-454.

Burns, S. (1998) "Easy Money", *Accountancy*, August: 38.

Comer, M.J. (1998) *Corporate Fraud*, 3rd edition. Network Security Management Ltd.

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*. European Communities.

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.

Fraud Advisory Panel (2002) *Fighting Fraud - A guide for SMEs*. London: FAP.

Higson, A. (1999) *Why is management reticent to report fraud? An exploratory study*. London: FAP.

Johnson, G. (1992) 'Managing Strategic Change - Strategy, Culture and Action', *Long Range Planning*, 25(1):28-36.

Appendix

Altogether sixteen interviews took place between November 2000 and June 2001. Three pilot interviews were conducted, followed by thirteen main interviews. One organisation was represented at both the pilot and main stage, and one interview contained representatives from two organisations. I am grateful for the co-operation of individuals from the following organisations:

Andersen
Audit Commission
Baker Tilly
Defries Weiss
Deloitte & Touche
District Audit
DTI
Ernst & Young
HLB Kidsons
KPMG
Kroll Associates
Kroll Lindquist Avery
London Metropolitan Police Fraud Squad
Kingston Smith
Robson Rhodes
DBO Stoy Hayward

This does not mean that the above organisations necessarily endorse the findings of this study.

Fraud Advisory Panel

For a printed version of this document or for information about the Fraud Advisory Panel, please contact Helen Fay by e-mail on

Helen.Fay@icaew.co.uk

Or write to

The Fraud Advisory Panel
Chartered Accountants' Hall
PO Box 433
Moorgate Place
London
EC2P 2BJ

Useful Organisations

Serious Fraud Office
Tel No: 020 7239 7272
www.sfo.gov.uk

City of London Police Fraud Squad
Fraud Desk Tel No: 020 7601 2222
www.cityoflondon.police.uk/level1/crime/fraud_main.html

Metropolitan Police Fraud Squad
(for high value fraud involving amounts of at least £750,000)
Tel No: 020 7230 1212
www.met.police.uk/so/so6.htm

National Criminal Intelligence Service (NCIS)
Tel No: 020 7238 8431
www.ncis.co.uk

Financial Services Authority
Tel No: 020 7676 1000
www.fsa.gov.uk

Confederation of British Industry
Tel No: 020 7395 8195
www.cbi.org.uk

Department of Trade and Industry
Tel No: 020 7215 5000
www.dti.gov.uk

Companies House
Tel No: 0870 333 3636
www.companieshouse.co.uk

National Audit Office
Tel No: 020 7798 7000
www.nao.gov.uk

Institute of Chartered Accountants in England & Wales
Tel No: 020 7920 8100
www.icaew.co.uk

Law Society
Tel No: 020 7242 1222
www.lawsociety.org.uk

Home Office
Tel No: 020 7273 4000
www.homeoffice.gov.uk

Public Concern at Work
Tel No: 020 7404 6609
www.pcaw.demon.co.uk

Small Business Service
Tel No: 0114 259 7788
www.businesslink.org

The Fraud Advisory Panel
Chartered Accountants' Hall PO Box 433 Moorgate Place London EC2P 2BJ **www.icaew.co.uk**