

# **A Short Guide to Fraud Risk**

Fraud Resistance and  
Detection

*Martin Samociuk and Nigel Iyer*

*Edited by* Helenne Doody

**GOWER**

# 1 Managing Fraud Risk

Spectacular corporate collapses and numerous major frauds in recent years have sharply focused the minds of company directors, owners and regulators on the need to understand and manage fraud risk. This guide explains what fraud risk is and how, in practice, you should deal with it. We are going to assume that, in reading this book, you are someone who would like to contribute to successfully managing fraud risks in your organisation. You may have a different role, such as Finance Manager, Procurement Officer or Internal Auditor, but for the purposes of this book, we will refer to you as the 'Fraud Risk Manager'.

We appreciate that you most likely are not the Chief Executive Officer ('CEO'). CEOs rarely have the time to take a direct interest in fraud risk management and usually assign this role to others, such as the Head of Corporate Security, Operational Risk, Internal Audit or a dedicated Fraud Officer. Nevertheless, even though they may have assigned responsibility elsewhere, the CEO, together with the Chairman of the Board ('Chairman'), should still act as a direct, pivotal role model for

the rest of the organisation when trying to manage fraud risks. We discuss why this is so important in Chapter 2. We use the term 'Board' as meaning the management board comprising the executive and non-executive directors.

Successful management of fraud risk does not solely depend on implementing controls and procedures. It also requires the Board to support initiatives and policies for developing an anti-fraud culture and needs Executives, Business Line Managers and employees to understand their fraud risks. The Fraud Risk Manager can help to facilitate this.

Why is understanding fraud risk so important? Looking at the many corporate collapses caused by fraudulent behaviour, a hallmark of the victim organisations was that they had not understood fraud risk. With more foresight, could they have anticipated and prevented the loss or are frauds impossible to predict?

We believe that a large part of the problem probably lies in the way that fraud risks have been assessed, treated and reported (or not). Hence we have devoted a whole chapter to fraud risk assessment (Chapter 3) and a chapter to treating and reporting fraud risks (Chapter 4).

But before we start, let us explain what we mean by the term 'fraud risk'. First, it is important to define 'fraud'. There is no universal definition and we will use the definition 'using deception to make a personal gain dishonestly for oneself and/or create a loss for another' (CIMA 2009). Plainly speaking, fraud involves a perpetrator committing a deceptive act to obtain a benefit.

Therefore, fraud risk is the chance of a perpetrator (or perpetrators) committing a fraud which has an impact on the organisation. Fraud can occur anywhere where there are people who are dishonest, or who become dishonest.

*Key Point: a fraud risk comprises three elements:*

- 1. the method of fraud;*
- 2. the effectiveness of controls;*
- 3. the degree of dishonesty and skill level of the perpetrator.*

The impact or consequence of fraud can be both positive and negative to the organisation's interests. For example, managers working in the interests of the company may fraudulently evade paying corporation tax. Similarly, financial market traders may fraudulently take profits from customers to improve their own results and therefore also the profits of the organisation they work for. The financial impact is temporarily positive, but the reputational impact (and consequential costs) if the fraud comes to light is probably going to be somewhat negative.

We have found that one of the main reasons people do not understand fraud risk is that they sometimes focus too much on the method of fraud and not enough on who might be doing it and why. This tends to happen when an organisation has a risk management framework which requires managers to assess fraud risks alongside other risks using a 'one-size fits all' assessment process with the main focus on controls.

It is important to remember that frauds are not accidents. They are deliberate acts and it is people who are committing them. Given the different nature of fraud risks compared with other risks, such as credit and market risks or risks resulting from accidental occurrences, fraud risks should be assessed independently of the general risk assessment process. We will come back to this message throughout this guide and we will provide more detail on how to assess fraud risks in Chapter 3.

## **GETTING STARTED**

So assuming you would like to be involved in developing and implementing strategy to manage fraud risk, where do you start?

You may not be in a position to issue policies or set a budget on your own, so getting the Board and other powerful internal allies on side is critical. Once a workable policy has been approved and issued, all line managers should be required to analyse fraud risks in their business unit and put in place anti-fraud controls and procedures.

However, successful fraud risk managers do not stop here. They understand that effective fraud prevention is as much about culture and ethics as it is about policies, starting right at the top with the Chairman and CEO. Fortunately, most organisations that we have dealt with over the last 25 years have had honest and ethical Chairmen and CEOs. In this case, it should be reasonably straightforward to get support to implement a strategy from the top down, especially when you demonstrate that reducing fraud can improve profit margins. We do not want you or your CEO to get too excited,

but effective fraud risk management could mean more than a 60 per cent increase in profits, as we show later.

If you are unfortunate enough to work in an organisation where the culture is dominated by executives with a poorer-than-average sense of ethics, then your own situation is more complicated. As discussed further in Chapter 2 'Developing an Anti-Fraud Culture', there are sadly examples of executives who use policies and governance as a smokescreen to reassure their investors and the outside world the organisation is ethical and well controlled, while in the meantime they indulge in unethical or criminal behaviour for their own personal gain.

You can still try to make a difference within such an organisation, but it may be a difficult, if not impossible task, particularly if you cannot get buy-in at the Board level. If that does not sit well with you, in the following chapters we discuss some of the red flags which may give you an indication as to the sort of executives you are working for, so that you can think about whether or not you want to stay within that organisation or change to a more ethical employer. If you do choose to stay in an organisation with a 'challenging' environment, then it will help if you can find support from at least one Board member.

*Example: A Chief Financial Officer ('CFO') uncovered a corrupt relationship whereby a Senior Purchasing Manager had received a shipment of concrete at his home address from a supplier which had won a tender for a construction project for the company. The concrete was used to build a new driveway. However, the CEO decided to take no further action because the supplier had a long-established relationship and had successfully delivered*

*on a number of projects. There was no suggestion of a corrupt relationship involving the CEO.*

*The CFO was unhappy with the decision and notified the Chairman who agreed that not taking any action would set entirely the wrong tone throughout the organisation. After a showdown with the CEO, the Chairman obtained the backing of the majority shareholder to overrule the CEO. The supplier relationship was terminated and this information was made public both within the organisation and across the industry. The Chairman reasoned that setting the correct tone would act as a deterrent for any future improper relationships. However, it took a determined effort to repair the relationship between the Chairman, CEO and CFO.*

The level of support which the executives provide to a Fraud Risk Manager will depend largely on their own experiences. The more fraud they have seen, the more risk averse and supportive they will often be.

We will now cover the main elements of a fraud risk management strategy and then discuss three issues which you should understand.

## **THE FRAUD RISK MANAGEMENT STRATEGY**

Aside from an organisation's own desire to manage fraud risk, there is increasing pressure from national and international legislative bodies for organisations to implement a fraud risk management strategy. A good place to start for a Fraud Risk

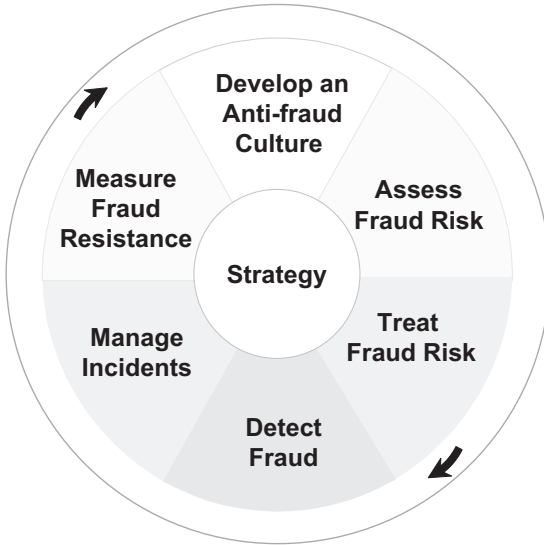
Manager wishing to implement a strategy is to look at any previous cases of fraud, both internal and external to the organisation, and draw up a list of the major elements which should be in place to reduce risks of similar events reoccurring. For example, analysis of the spectacular losses in the US during the banking crises of the 1980s and early 1990s, when more than 1,600 banks were closed or received financial assistance, the Barings Bank-type trading frauds in the late 1990s and early 2000s, and the equally spectacular losses in the late 2000s reveals some common factors:

- the fraud risks were not fully understood;
- management supervision was poor;
- weaknesses in internal controls were not identified;
- red flags and fraud warnings were ignored;
- honest and innocent people had closed their minds to the possibility of fraud.

An effective fraud risk management strategy should consider all of these factors and treat the identification and reduction of fraud as a separate part of an organisation's overall risk management strategy.

The fraud risk management strategy should consist of six elements as shown in Figure 1.1.

Each of the elements is discussed in the following chapters. Together they are designed to manage the risk of fraud across the whole organisation – starting at the top, with the Board,



**Figure 1.1** Fraud risk management strategy

which has the broad picture of where the high-level risks are likely to be, down to individual operating units, which should be able to produce detailed fraud profiles.

Some organisations may already have a fraud risk management strategy in place. We believe that taking the approach advocated in this book will enhance traditional fraud risk management and make organisations more resilient to fraud. The objective is not necessarily to reduce every fraud risk to zero; just being in business carries a risk of fraud. The aim is to prevent high-impact frauds and reduce the hidden costs of fraud, whilst implementing a minimum number of controls to enable the business to function efficiently. Some organisations may choose to accept or tolerate some low-impact fraud risks because it is neither cost-effective nor practical to eliminate the risk completely. At the same time, it is possible to design and

implement procedures to deter potential fraudsters, including methods to spot those frauds which do occur and policies for dealing with perpetrators. For example, some organisations have a 'zero tolerance' approach, which means they will take action against anyone who has committed a fraud, regardless of the financial loss involved or the position of that person within the organisation.

A fraud risk management strategy is designed to assist executives in developing a fraud resistant organisation – in ways that can be more readily measured and compared to other organisations.

To ensure that the Board fully support the strategy, there are three main issues which they should understand and accept. These are:

1. the real cost of fraud;
2. the 'changeable' nature of honesty, and the need to draw a line for employees;
3. how the motivation to commit fraud varies both from person to person, and is influenced by time and circumstances.

If the Board has a poor understanding of these issues, it can adversely influence the way they perceive fraud risks and hence the support they provide for implementing the strategy. If you are going to participate actively in implementing the strategy, we have found an effective way to raise these issues is to measure the perceptions of line managers (discussed in Chapter 4) and then, depending on your reporting line,

present the results to senior management or direct to the Board as part of a fraud briefing.

## THE REAL COST OF FRAUD

It is important that the Board recognises the real cost of fraud and understands that investing in fraud risk management can have a positive impact on profits. There can be a tendency for Boards only to offer adequate support and attention to fraud risk management following the discovery of a major fraud. At that stage executives can see with the benefit of hindsight where problems existed that allowed the fraud to take place. They are then keen to implement a wide range of controls to prevent a reoccurrence and more readily allocate resources and funding.

This hindsight approach to fraud risk management is common because there has been little training at the executive level on how fraud can impact an organisation. Few MBA programmes pay much attention to the prevention of corporate fraud, give or take the occasional mention at a business ethics lecture. The same goes for graduate and other training programmes aimed at budding executives.

*A Personal Experience: At an initial meeting with a professor who led a well-regarded Executive MBA programme, the first question he asked was: 'Why do you want to see me about fraud?' I asked him what the main subject he lectured in was and he responded: 'Risk Management'.*

*I asked him to name his favourite three books on risk management. At this, he extracted three titles*

*from the overflowing shelves in his office. In turn, we scoured the index of each book for the words 'fraud', 'corruption', 'malpractice', 'embezzlement' and other related terms. None of the words were listed. The professor then asked me about the significance of my demonstration. I went over to his desk and picked up a number of that day's newspapers. Each of the front pages had stories of companies or government bodies being damaged by fraud and corruption, and there were other similar stories on the inside pages. The professor saw the point. Fraud is a key risk to business and it is unwise for risk management programmes to ignore this.*

Although business schools are changing, these changes will take some time to filter through to upper management. In the meantime, there is a wealth of academic and empirical research which demonstrates the extent and effect of corporate fraud, which can be used to help educate the Board. Most studies speak of the cost of fraud being in the range of 2–7 per cent of turnover. For example, research by the Association of Certified Fraud Examiners (ACFE 2002–2008) in the US across a wide range of industries has repeatedly indicated that:

- fraud is a widespread problem that affects practically every organisation;
- the typical organisation loses 5–7 per cent of its annual revenues to fraud.

Surveys indicate there is general agreement within different industry groups that fraud losses are significant. However, when we visit individual companies and speak with senior managers, they frequently argue that their losses are a small

fraction of the industry averages. It is as if everybody feels that they are a special case and are not affected as badly as other companies.

In most cases the hidden indirect costs of fraud, such as constraints on expansion and development, damage to reputation and employee morale, greatly outweigh the direct costs. Also, the indirect costs of an investigation can be significant, sometimes even as much as the amount lost, or more. Another important indirect cost is in the large amount of time which managers have to divert to dealing with the issue. Arguably, the greatest and most ignored indirect cost is the cost of all the ongoing frauds which have not yet been discovered.

The ability to increase profit margins is one compelling reason to systematically manage fraud risk. If the cost of fraud in a company was say 3 per cent of sales (and this is a conservative estimate based on the ACFE figures of 5–7 per cent) and the current operating profit margin was say 5 per cent, then removing fraud from the organisation would result in a 60 per cent increase in profit margin, as illustrated in Figure 1.2.

Phrases like ‘one way of making money is to stop losing it’, ‘it’s not a problem, it’s an opportunity’ and ‘prevention is better than cure’ have all been overused in business. However, in the context of fraud, they are indisputably true.

Even where an organisation’s cost-base is continually under scrutiny, management rarely look for hidden costs related to fraud.

|                      |                |                                  |
|----------------------|----------------|----------------------------------|
| Sales                | 1000           |                                  |
| Costs                | <del>950</del> | 920 *                            |
| Operating Profit     | <del>50</del>  | 80 *                             |
| <hr/>                |                |                                  |
| <b>Profit Margin</b> | <b>5%</b>      | <b>8% *</b><br>(60% increase!!!) |

\* If fraud and corruption = 3% of sales

**Figure 1.2 Hidden costs**

*Example: A multinational company recruited a new internal Training Manager to bring in fresh ideas to its management training scheme.*

*The new recruit immediately brought in some purportedly world-renowned management consultants. In order to pay these consultants, it was necessary to displace (or make redundant) some of the employees in the training department.*

*It was subsequently discovered that the renowned consultancy was in fact one person who used a number of low-paid sole traders working out of his remote farmhouse. At least 80 per cent of the \$2 million invoiced by the head consultant was found to be fictitious. To keep the internal manager happy he had arranged payment of his divorce settlement, given him a car and paid for several holidays. It turned out that the consultant and the training manager had been involved in a similar scheme at a former employer. A*

*post-mortem review concluded that it was all too easy for senior managers to approve project budgets like this for areas in which they were the specialists, without being adequately challenged. In total over 200 similar senior managers had the same opportunity to abuse their budgets without this being detected.*

Rather than discover the cost of fraud post-event, we believe that most executives would prefer to understand the potential losses and prevent the money going missing in the first place. This can be achieved by conducting fraud risk assessments, treating the risks and then reporting risks which remain unacceptably high to the Board.

## **THE VARIABLE NATURE OF HONESTY**

The second topic to explore with executives is whether they appreciate that each individual has their own level of honesty, both on a personal level and at work. An organisation cannot afford to let employees set their own level of honesty at work, as this may be out of step with what the employer expects. Hence an organisation should draw a line as to what is acceptable and unacceptable behaviour in the workplace.

When executives have not experienced fraud, they sometimes naively believe that all people around them are honest and that employees know where to draw the line. As a result, they may be reluctant to believe that fraud can happen in their organisation.

What they do not realise is that the word 'honesty' can be interpreted very differently. Honest behaviour to one person could be seen as dishonest by another. Unless somebody in

the organisation clearly sets out what is honest or dishonest, then each employee will have their own interpretation. For example, you probably think that you are honest (and hopefully you are!), but how honest are you? Try this test to assess your level of honesty.

**Table 1.1 Perception of honesty**

| <b>Question</b> | <b>Have you ever...</b>  | <b>Your answer<br/>(Y/N)</b> |
|-----------------|--|------------------------------|
| 1               | Illegally copied software, music or movies?  |                              |
| 2               | Travelled on a bus or train without paying the fare?   |                              |
| 3               | Used office stationery or equipment for personal use whilst at work or taken it to use at home?                  |                              |
| 4               | Knowingly inflated a private insurance claim?  |                              |
| 5               | Paid invoice-free cash to a builder, plumber, electrician, etc?  |                              |
| 6               | Deliberately exceeded the speed limit?   |                              |
| 7               | Added things that you should not have to a travelling expenses claim?  |                              |
| 8               | Claimed a benefit that you did not really qualify for?   |                              |
| 9               | Told a 'white lie' about your qualifications?  |                              |
| 10              | Not paid a parking fine?   |                              |
| 11              | Received and not declared a gift from a supplier or customer?  |                              |
| 12              | Made a 'facilitation payment' to get a contract or win business when it really could have been called a 'bribe'? |                              |
| 13              | Stolen anything, even of a low value?  |                              |
| 14              | Submitted personal expenses such as golf club membership or private entertainment as a company expense?          |                              |

**Table 1.1      *Concluded***

| Question | Have you ever...   | Your answer (Y/N) |  |  |
|----------|--|-------------------|--|--|
| 15       | Channelled company purchases or services through another company in which you or your family members have a personal interest? |                   |  |  |
| 16       | Under-stated or left out items from your tax return?   |                   |  |  |
| 17       | Brought items through customs which you should have declared?  |                   |  |  |
|          | YOUR SCORE   | YES               |  |  |

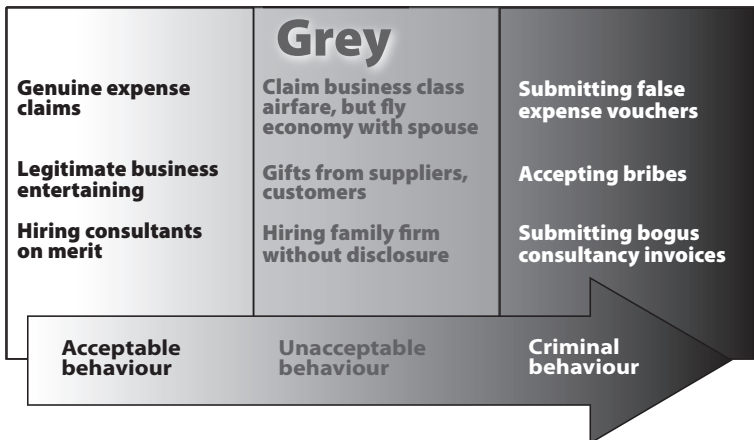
If you were totally honest in replying, how did you do?

Typically people can answer ‘Yes’ to five or more questions and yet still think of themselves as fundamentally honest. We have to accept that nearly everyone bends the rules, given the opportunity and their own motivation. The degree to which people bend the rules will also depend on individual personalities. For example, CEOs are natural risk takers and hence seem to be willing to bend the rules more than others. It is common to find a CEO will answer ‘Yes’ to more than five questions, whereas more cautious individuals such as Accountants or Human Resource Managers will usually answer ‘Yes’ to less than five.

Try the test with your executives or with any other group of people, as an anonymous questionnaire, explaining that the answers will be shredded afterwards and not retained. If you conduct the survey with a large number of employees, you will probably find that there are very few instances when someone answers ‘No’ to all the questions. When it does happen, it is usually for cultural reasons, for self-protection or because of embarrassment.

It is up to the organisation to draw the line on what is considered acceptable and honest behaviour within the work environment. Some companies recognise that employees may bend the rules, for example, by taking the odd pen or piece of stationery home. Such practices are usually accepted. However, where no clear line is drawn for employees, it can develop into wholesale removal of boxes of materials to sell privately. Then, a minor bending of the rules becomes a more serious fraud.

The progression can be an almost unnoticeable process. Usually employees do not realise that they have crossed the lines between acceptable and unacceptable business behaviour, and perhaps then between unacceptable business behaviour and criminality. As shown in Figure 1.3, the progression from acceptable to unacceptable to criminal behaviour can be a seamless transition for some employees because they do not see, or they choose to ignore, where the line is.



**Figure 1.3** Shades of grey

Employees are sometimes naïve or ignorant of the consequences of their action. They do not realise the seriousness or criminality of what they are doing nor are they aware of the heavy penalties. For example, where bribes have been received, employees may believe they have been given a gift in exchange for doing a favour for someone, which in fact benefits their own company. When discovered, such employees argue they did nothing wrong because company policy defining acceptable or unacceptable behaviour was unclear.

It is also important to consider that ‘acceptable’ behaviour may vary across national borders; multi-national organisations should be clear about what is acceptable in all countries in which they operate. We will discuss this further in Chapter 2.

## **THE VARIABLE NATURE OF MOTIVATION**

The third issue which executives should understand is that motivation to commit fraud varies and a person’s motivation can develop over time, sometimes very rapidly. Some executives, particularly those who promote an ethical and honest workplace, find it hard to accept that people with certain personalities have a strong tendency to be dishonest and that even employees who are normally honest could one day be tempted.

Fraud and corruption takes place because an individual or group:

- sees an opportunity to make money or obtain other benefits and believes they can get away with it;

- is motivated to act;
- can justify or rationalise their actions.

These factors are sometimes summarised in a model referred to as the Fraud Triangle (CIMA 2009).

If asked to think about it, most honest people are usually able to spot opportunities to commit fraud. They can also usually work out a method whereby they believe they will not get caught. However, because they are honest, they believe that they will never take advantage of that opportunity. For some though, the day may come when their circumstances change in a way that provides them with the motivation and the ability to justify fraudulent activity.

*Example: An IT manager in a Scandinavian bank changed from being honest, hard working and potential senior management material to a fraudster within the space of 12 months. His new girlfriend was addicted to heroin and managed to get him addicted as well. Despite the fact that he had taken fraud prevention courses and knew all about avoiding detection, he was so desperate for money that he simply started crediting his girlfriend's account using false internal vouchers which were quickly detected.*

*A more extreme example: You have young children. You also hold the access keys to the company's payment systems. If a criminal group kidnapped your children and told you they would be returned in exchange for giving them the keys, would you cooperate? Everyone we have asked this question has answered yes.*

Thankfully, the scenarios in the examples are not common. However, it often does not take such extreme pressure for people to cross the line between honesty and dishonesty. A popular example of senior executive dishonesty is described in the book *Freakonomics*. In the so-called ‘bagels test’ (Levitt and Dubner 2005), when a basket of bagels was placed in corporate offices along with an honesty box for payment, it was discovered that, more often than not, executives higher up the corporate ladder did not put money in the box, whereas lower-level employees were typically honest.

Sometimes executives (and consequently some employees) convince themselves that certain frauds are in fact beneficial for the company. Common examples include:

- payment of bribes to win contracts;
- smoothing or inflating of sales figures, profits and/or assets;
- hiding bad debts or obsolete stock;
- moving funds into and around offshore destinations to avoid taxes;
- price fixing or the establishment of cartels;
- circumventing export embargoes;
- submitting lower valuations to avoid customs duties;
- avoiding VAT and other taxes;

- overcharging clients;
- obtaining subsidies and grants on false or partly false premises.

All these things probably increase profits and shareholder value. It makes it easier to justify fraud when it is perpetrated in the best interests of the company, its shareholders and employees. Experience has shown that such attitudes are short-sighted and often lead to more widespread fraud or, like many high-profile examples, complete collapse.

Unfortunately, it is not possible to draw up a personality profile of the typical fraudster that could be used to pre-empt a fraud. Over the last 25 years, we have investigated fraud at all levels within organisations, involving both male and female employees, and, so far, we have not found any set of reliable indicators that one could use to accurately predict whether someone was going to become a fraudster. Sometimes, it is very difficult to understand the motivation of someone who participated in a fraud.

*Example: In Operation 'Wooden Nickel', the FBI arrested 47 foreign exchange traders in New York. The traders had colluded to defraud customers by quoting off-market rates and passing the profit (usually a few thousand dollars) down the chain to a bank account, where the money could be withdrawn in cash and distributed amongst the participants. In some cases, individuals received a few hundred dollars cash on the deal. Whilst the traders have not revealed the reason why they colluded, given the sizeable salaries and bonuses which these traders were earning,*

*the motivation does not appear to be the monetary reward.*

*We have spoken to some other traders about this case and the consensus seems to be that they may have done it just because they got a kick out of taking the risk.*

One personality type which seems to have a much higher motivation to commit fraud is the type known as the ‘corporate psychopath’ (Clarke 2005). A Canadian psychologist, Dr Robert Hare, identified the following eight traits to try to define a corporate psychopath (Hare 2003):

- glib and superficially charming;
- grandiose sense of self-worth;
- pathological liar;
- very skilful manipulator;
- lack of remorse;
- displays shallow emotions;
- callous and lacks empathy;
- fails to accept responsibility for his or her own actions.

Individuals with these traits can reach the highest levels in an organisation and can wreak untold damage. Interestingly, there is very little to distinguish this type of person from

those in the upper echelons of organised crime. However, few human resources departments are equipped to screen for this personality type prior to employment and corporate psychopaths are very good at hiding their true characters once employed.

Hare emphasised that a person displaying some of the characteristics is not necessarily a corporate psychopath: there needs to be a cluster of related symptoms. However, a look back at the character of some of the CEOs and other executives responsible for major corporate collapses raises some interesting questions. Corporate psychopaths have an overwhelming urge to obtain the power and status that having a lot of money brings. They desire influence and power over their colleagues, make plans over long periods of time, and are able to lie, deceive and manipulate as required without feeling any remorse.

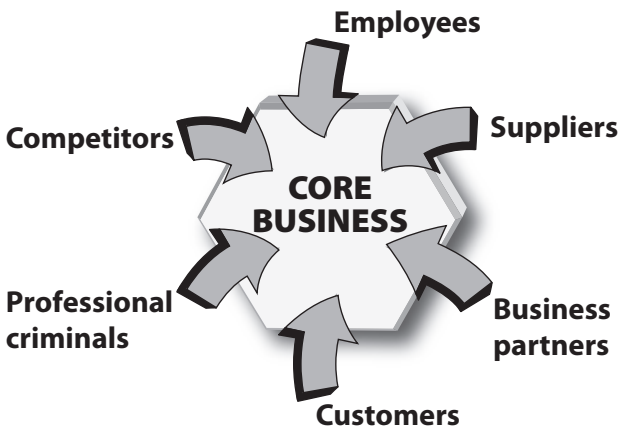
Very few people actually see the real persona though. Most usually see the executive as someone who has to be tough to do their job, or as a suave, charming and intelligent person. Only those few who are on the receiving end of the corporate psychopath's attention may catch a glimpse of what is lurking below the surface.

People with psychopathic traits have no qualms about manipulating honest employees. For example, there have been many cases where con artists, posing as customers, have convinced honest employees in a call centre to reveal confidential customer information, or persuaded a back-office person to move money out of a customer's account. In these cases, it usually comes as a complete shock to the employee that they have been duped. They believed they were only

helping the customer. That is why even companies with very good controls can still suffer from fraud: because their own honest employees choose to bypass the controls in favour of providing better customer service.

Much traditional thinking about fraud tends to focus on dishonest employees. However, employees are just one of a whole range of potential perpetrators. Employees often have to take quite high risks for a relatively low reward. On the other hand, external parties such as fraudulent suppliers, business partners, customers, competitors or professional criminals can often take much lower risks for much greater rewards. The truth is that nearly everyone involved in or associated with an organisation could be a potential fraudster (see Figure 1.4 below).

Once there is collusion between employees, or between employees and an external party, fraud is much harder to stop. Unfortunately, this is a growing problem. As well as corrupting existing employees, criminal groups now actively



**Figure 1.4 Who commits fraud?**

seek to place their own person in a company as a temporary employee or contractor. Once a fraud starts, honest employees can then be drawn in as a dishonest culture develops.

*Example: The main board of a multinational organisation appointed a new management team at a subsidiary which had been grossly underperforming. The new management received a tip-off from a young former employee that fraud was rampant throughout the organisation.*

*A covert investigation uncovered a multi-million dollar fraud involving almost the entire salesforce with payments moving upwards to a senior manager reporting to the new executives. It came out during the trial that honest employees were actively encouraged to join in the frauds or were intimidated into leaving the company, for example by having their cars vandalised. In the end 14 people were convicted, with a large number of other employees and managers being dismissed.*

Even though they believe that employees may be honest today, prudent managers should prepare for the possibility that one of their employees, suppliers or other third parties could become dishonest in the future.

In the same way that a person's motivation is dynamic, organisations are dynamic, and new opportunities present themselves as a company evolves. For example, rapid expansion into new territories, implementation of new IT systems, or cost cutting and reduction in head count can all raise or lower fraud risks. The fraud risk assessment process should be flexible enough to cater for these changes as discussed in later chapters.

## SUMMARY OF POINTS

- Fraud is ‘using deception to make a personal gain dishonestly for oneself and/or create a loss for another’.
- A fraud risk is the chance of a perpetrator (or perpetrators) committing a fraud which has an impact on the organisation.
- A holistic fraud risk management strategy is designed to assist senior management build a fraud resistant organisation.
- People commit fraud. A method of fraud is not a risk until it is linked to a person or persons who can make use of it i.e., to a perpetrator or perpetrators.
- A successful fraud risk management strategy relies on the board recognising the cost of fraud and on raising awareness of fraud risks across the organisation.
- It is now widely accepted by fraud prevention professionals that fraud is a hidden cost carried by most businesses and may be as much as 5–7 per cent of turnover.
- The total cost of fraud can greatly outweigh the direct financial loss.
- Systematic management of fraud risk can significantly increase profit margins; stopping losses from fraud adds directly to the bottom line.

- Executives who have not experienced frauds tend to overestimate the honesty of their workforce and underestimate the fraud risks.
- Changes in personal circumstance, which the Board cannot control, can motivate even honest employees to perpetrate fraud.
- People demonstrating traits of a corporate psychopath can have a positive need to commit fraud.
- Prudent managers should prepare for the possibility that one of their employees, suppliers or other third parties could become dishonest in the future.
- Clear boundaries should be drawn between acceptable and unacceptable behaviours.