A risky business…

…In spite of the fact that it's one of the key risks to be managed, a great many corporations ignore the tangible threat posed to their operations by fraud. So what are the appropriate countermeasures that will mitigate the risks involved?

Traditionally, the practice of risk management comprises acceptance, transference, elimination, control, sharing, insurance – and the avoidance of a diverse array of risks. Risk management and internal control business models have subsequently been devised which cater for all eventualities, categorised by terms such as business, operational and reputational risk. How, though, does fraud perform as a risk, and where exactly does it fit into the risk management hierarchy? Fraud is very much the corporate 'F' word. It doesn't appear in any management best sellers, in MBA courses or as part of [security] management training and consultancy.

Business is awash with 'best practice' techniques on generating and maximising profit, but woefully lacking in knowledge of how to minimise and manage losses. And, as has become all-too-evident in recent years, a single fraud can wipe out years of profit, drive away investors, ruin a brand or even bankrupt the largest organisation.

Managing the risk of fraud

The practice of fraud risk management includes fraud prevention, deterrence, disruption reporting, detection, examination, investigation, enforcement and recovery. These are all well-defined and well-honed disciplines in their own right, each with laudable objectives.

However, they're seldom embedded in an organisation's culture, or given significant management support to succeed. Rarely are they used in tandem, and all-too-often the investigation of fraud manifests itself as a knee-jerk reaction to a problem that's badly out of hand. Sometimes merely for the want of basic controls.

Business is awash with 'best practice' techniques on generating profit, but lacking in knowledge of how to minimise losses.

Until recently, there existed few guidelines to underpin the implementation of fraud risk management. Thankfully, this position has now changed, insofar as corporate governance initiatives have provided a framework for financial controls in a financial reporting environment. That said, the framework for these models assumes that fraud is a business risk to be managed in the same way as any other business or financial risk.

If an organisation accepts that it could be exposed to fraud and, let's face it, absolutely no organisation is immune to it – then that firm (and in particular its security and IT specialists) needs to specifically address the subject of fraud prevention and control. Given the diversity and globalisation of fraud, putting in place comprehensive fraud countermeasures will take a given organisation a long way down the road towards accomplishing its usually long list of so-called 'corporate governance objectives'.

Putting your plan in place

Any fraud prevention and control model should aim to achieve one (or all) of the five primary objectives. These objectives are as follows:

- Prevention: stop incidents of fraud occurring;
- Deterrence: deter potential fraudsters from even attempting to perpetrate any fraudulent activity;
- Disruption: make life as difficult as possible for the fraudster – keep them on the move and under pressure;
- Identification: a good fraud prevention strategy will help to identify high risk activities and weaknesses in the control environment;
- Civil action/criminal prosecution: effective strategies will reduce the likelihood of needing to resort to costly civil actions or time consuming – and potentially disruptive – police investigations.

At the outset, consider fraud risk as an integral part of an overall corporate risk and security management strategy.

Fraud is every bit as much of a threat to any organisation as changes in legislation, competitor action or indeed inflation. Its overall effect then needs to be fully understood and managed accordingly.

Attempt to develop an integrated strategy for fraud prevention and control. Every organisation should possess this capability in order to draw all of the elements of the strategy together in forming an holistic and complementary raft of fraud countermeasures. Those organisations with a strategy are far less likely to suffer catastrophic losses from fraud than those without.

Ian Johnson Associates Limited (IJA) - Linden Place - Seale - Farnham - Surrey - GU10 1HS.
Tel: (+44) (0)1252 782664 **Fax:** (+44) (0)1252 782818. **Email:** info@ija.co.uk **Web:** www.ija.co.uk

Security teams and senior management must also develop an 'ownership structure' which cascades downwards through the organisation. Fraud prevention is everyone's responsibility, of course, but management acceptance and ownership is essential if the strategy is to work. Specific ownership responsibilities may also be placed on individual managers, or on the internal audit department.

Introducing a fraud policy statement is crucial. The statement should emphasise an organisation's attitude to fraud in its many guises, its determination to combat and prevent fraud and a commitment to punish those found guilty of wrongdoings. It should be simple, focused and easily understood by all members of staff. This is really the foundation stone of any organisation's fraud prevention strategy. An ethics policy is equally important. Directly supporting the fraud policy statement, this should be a code of business conduct emphasising the norms and values expected in daily activity.

Introducing a fraud policy statement is crucial. The statement should emphasise an organisation's determination to combat and prevent fraud.

It may spell out an organisation's approach to the payment of bribes, 'commissions' or 'management fees' (often relating to overseas business ventures), and ensures that all staff are aware of what's expected of them. All of this effort could come to no avail if no one knows about the policies. Staff cannot be made accountable for fraud prevention unless they are made fully aware of its importance, and the benefits arising from it.

Consideration should also be given to issuing personal copies to all members of staff, and to those with whom your organisation does business. This ensures that customers and suppliers know exactly where the company stands on fraud and ethical issues.

Establishing the control environment

Establishing a sound control environment requires a positive approach from all concerned. It's very easy to become sloppy and take short cuts. Security management philosophy and operating style are important factors, as are the appropriate organisational structures and adequate staffing levels. In fact, senior management must lead by example, and provide the right direction.

Meantime, setting up operational control procedures requires the documentation and execution of policies developed by managers to counter all identifiable risks.

Examples of this would include authorisation controls, segregation of specific duties, physical security measures and control over business transactions.

Education and training is all-important. All members of staff should be made aware of the general risk of fraud, whether the threat be internal or external. Specific threats facing staff in the workplace must be pinpointed, in particular those affecting their own job function (e.g. personnel, procurement or sales). Thereafter, staff must be trained to identify and respond to threats as and when they arise.

As far as introducing a so-called 'whistleblowing' policy is concerned, this must clearly indicate that senior management and the security team positively encourage people to come forward and report any instances of fraud and/or malpractice. It should emphasise that protective legislation is now in place, and allow for 'anonymous' reporting if a member of staff so desires.

A telephone reporting 'hotline' is an obvious add-on to this last measure, a direct line to that member of the security team dedicated to, or directly responsible for, fraud prevention. Such a service could actually be 'brought-in' increasing anonymity levels for staff members still further.

Policies and procedures can become obsolete very quickly. It's worth noting that, in many cases, it's actually the control system that's the first to go in the event of operational changes.

It may sound obvious, but policies and procedures can become obsolete very quickly. It's well worth noting that, in many cases, it's actually the control system that's the first to go in the event of operational changes. Thus, fraud control procedures should always be revised after organisational restructuring, downsizing of the business or changes in the way that a company conduct its business. The same would also be true if a new computer set-up has been installed, or indeed there has actually been an incidence of fraud.

If you would like further advice on this subject or would like to speak to an advisor, call our consultants on 01252 782664 or alternatively email: info@ija.co.uk

An abridged version of this article appeared in Security Management Today.

Ian Johnson Associates Limited (IJA) - Linden Place - Seale - Farnham - Surrey - GU10 1HS.
Tel: (+44) (0)1252 782664 **Fax:** (+44) (0)1252 782818. **Email:** info@ija.co.uk **Web:** www.ija.co.uk