FOILING THE FRAUDSTERS WITH FINGERS IN THE TILL

Tight profit margins have focused fresh efforts on cutting costly fraud, as **Geoff Nairn** reports

FRAUD PREVENTION

■ Prevention is better than cure and that is certainly the case with fraud, which costs the UK an estimated £85 billion a year.

"Putting in place pre-emptive measures could make very significant improvements to the financial health and stability of UK plc," says Jim Gee, director of counter fraud services at BDO International, the accountancy firm.

UK businesses have finally woken up to the huge financial cost of fraud and the importance of prevention.

"There has been a big change in the past few years," he says.

Before, fraud was viewed almost as an act of God. Businesses hoped it wouldn't happen to them and, if it did, they would worry about it then. Now, fraud is viewed as a business cost that needs to be measured and managed to drive improvements to the bottom line.

That change of attitude has led to a much more proactive approach to preventing corporate fraud, says Mr Gee, who was recently sent to Zambia to look for fraud in a mining company.

The firm had no concrete evidence that fraud was occurring. Rather, it suffered from rising costs and wanted to see if fraud could be responsible for its shrinking bottom line.

Irrespective of the sector in which it operates, there are certain types of fraud that affect almost any business as they exploit weaknesses in the two "Ps", procurement and people.

There is a wide variety of procurement frauds. For example, dishonest suppliers may try to claim payment for goods or services that have not been delivered, or they may deliver goods that have not been ordered – office supplies are a favourite – and then invoice the company for the unwanted and overpriced goods.

New technology makes new types of fraud possible. Payment redirection fraud has become quite a problem with the growth of electronic payment methods. With this scam, a fraudster e-mails or phones the accounts payable department of a business passing themselves off as a legitimate supplier and requesting that payments be sent to a different bank account – that of the fraudster.

But how does the fraudster get the details of a legitimate supplier?

"The amount of information that is in the public domain is remarkable," says Howard Cooper, associate managing director of investigations at Kroll, a specialist in risk consultancy. Suppliers often list their customers on websites and in the building sector, where this scam is particularly prevalent, the names of sub-contractors are often displayed at building sites.

Many procurement-related frauds can be foiled through stricter policies and procedures.

"The people who approve invoices don't spend as much time as they should on the task," says John Smart, head of fraud investigation at EY, the accountancy firm.

While it is relatively simple to train staff to check all invoices and goods delivered rigorously, it is more difficult to spot frauds that involve a dishonest employee, so-called insider fraud.

Mr Smart gives the example of a UK transport business, whose IT manager set up various fictitious suppliers to invoice the business for non-existent IT products and services.

The IT manager was able to get away with the fraud for a considerable time because the fake invoices resembled those of legitimate IT suppliers and their prices were competitive, so they did not raise any suspicions.

The alarm bell finally rang when the business realised its IT budget had grown suspiciously large and the IT manager was dismissed.

"It was a clever scam," says Mr Smart, who was brought in to investigate the fraud. Amazingly, he discovered the IT manager had performed the same scam at his previous employment.

That suggests a major failing in the transport company's recruitment procedures. But Mr Smart says the weak link is often the references provided by former employers.

Even if an ex-employee was sacked for fraud, HR departments worry about the legal repercussions of disclosing that to a third party, particularly if the employer kept the fraud quiet and there was no criminal prosecution.

Mr Smart says future employers should always verify information on applications and they should try to speak to former employers directly, particularly if the position applied for comes with a lot of responsibility and trust.

Not even the most comprehensive systems and controls can prevent a rogue employee from perpetrating a fraud.

"It does not matter how strong you make the controls because, if someone really wants to, they can evade them," says Kroll's Mr Cooper.

But a lot of fraud is opportunist and relatively easy to minimise by enforcing authority limits, holding regular audits and, perhaps most importantly, creating a corporate culture in which fraud will not be tolerated.

CHECKLIST

TOP TIPS TO COUNTER STAFF FRAUD

TRAINING

Train employees to spot "red flags" that betray common types of fraud. Ensure they understand the consequences fraud can have on the business.

POLICIES AND PROCEDURES

Put in place clear policies and procedures dealing with fraud, bribery and whistleblowing, with examples of behaviour that is and is not permitted.

INCENTIVES

Be careful designing incentive schemes based on achieving targets as they can encourage employees to "bend the rules" to meet monthly sales targets and receive a bonus, for example.

PRE-EMPLOYMENT CHECKS

Always confirm a new recruit's employment history, education and referees. Don't forget to also carry out checks on temporary staff and consultants.

AUTHORITY LIMITS

Set thresholds for obtaining approval for expenditure, limits on gifts and expenses claims, and restrictions on employees' access to IT systems.

EMPLOYEE PERFORMANCE

If employees feel their accomplishments are not adequately recognised, they are more likely to turn a blind eye to a fraud – or commit one themselves.

A lot of fraud is opportunist and relatively easy to minimise by enforcing authority limits, holding regular audits and creating a corporate culture in which fraud will not be tolerated