Spot the difference

How can you tell the good guys from the bad guys? With fraud on the increase and the recession set to keep it that way for the foreseeable future, at least attempting to do so should be on all companies' agendas

The Serious Fraud Office's (SFO) workload is swelling in the recession. Since the overhaul following an investigation into its own operational and accounting procedures, the economic crime squad has investigated a series of high-profile cases, including a financial products inquiry into US insurer AIG, the failure of car manufacturer MG Rover and the UK operations of US fraudster Bernard Madoff. That overhaul resulted in a jump in successful prosecution rates to 78 per cent, with 17 out of 18 cases won in court.

This jump is not just down to changes at the heart of the crime squad, either, which will have its work cut out even more next year when its budget is cut and it has to deal with an even greater number of cases.

Speaking to the *Telegraph* in mid-July, SFO director Richard Alderman said: "I'm sure the economic crisis means we will see more cases. Many will have been made sharper by Madoff; started to ask 'where is my money?' and are not reassured by the answers."

The impact of fraud can be serious – from purely financial consequence to potentially the very survival of businesses. And no business type is immune.

Philippa Ellis, senior associate in the Dispute Resolution Group at Davies Arnold Cooper solicitors comments: "The recession has exacerbated the increase in fraud with individuals becoming increasingly desperate to subsidise their income to compensate for a reduction in earnings. Fraud is soaring with the number of reported cases having increased by 64 per cent in the last financial year.

"Insurance companies are always at risk of fraudulent claims by dishonest insureds and the downturn in the property market has resulted in an increase in mortgage fraud which continues to be particularly prevalent. Mortgage fraud is not only being perpetrated by individual brokers, but also by the deliberate over-valuing of new developments, which requires a conspiracy involving lawyers, estate agents, surveyors and developers."

Indeed, discussions are underway with the Solicitors Regulatory Authority, the National Society of Surveyors and the Council of Mortgage Lenders to try to prevent further frauds.

The inside threat

Whether its a headline-grabbing story or a relatively low-profile but equally damaging set of circumstances, the need for awareness of workplace fraud throughout industry is real and urgent. Accountant BDO Stoy Hayward indicates that employee

WORST CASE SCENARIO – THE INSURANCE PERSPECTIVE

While D&O providers should be expected to thrive in this environment, so too are those offering or broking fidelity or crime insurance. Fidelity insurance covers loss of property due to an employee's dishonesty, as well as suspicious loss of property that cannot be directly attributed to a particular employee. Wordings vary and much will depend on the exclusions that operate but it will generally be in insurers' interests for the perpetrators of fraud to be identified. That way, insurers who pay out under a policy will have a chance of recovering their outlay from the fraudsters directly.

In order to maximise their chances of recovery, insurers, loss adjusters and brokers might have regard to these ten tips:

1. Control very carefully who knows what about the internal investigation. Secrecy may be crucial but is difficult to secure where information is widely disseminated.

2. Consider whether injunctions need to be obtained against those believed to be in receipt of criminal property.

3. Private law injunctions can be expensive to obtain. In certain cases it might be worth contacting the police to see whether they would be willing to obtain injunctions under the Proceeds of Crime legislation.

4. It is important to consider carefully matters of timing. If insufficient investigation is undertaken before an injunction is sought, the fraudsters may be able to defeat the application, but will nonetheless be aware of the interest in them, and may flee the jurisdiction and take with them or hide their assets. If too much time is taken, then the risk of the action becoming known to the fraudsters is increased. Delay may also enable the courts to conclude that the injunction ought to be refused because there is no evidence that the claimant will be disadvantaged prior to a full trial of the issues.

5. In order to maximise the chances of recovery it is important to identify all those who may have aided and abetted the fraud. In a large number of cases, the dishonest employees will have colluded with contractors, customers or suppliers, perhaps benefiting from a kick-back.

6. Be careful where proof of the fraud largely turns on digital evidence. In such a case, consideration should be given to employing an IT forensics expert who can establish to a court's satisfaction that the evidence presented is a faithful record of electronic information contained in a digital device that was properly functioning at all material times.

7. Be aware of the company's obligations to the criminal and regulatory authorities. For example, some types of employee crime may involve the company in the commission of offences, in the underpaying of tax or duty, or to the overcharging of customers. Careful thought will have to be given to whether disclosures should be given to authorities and the timing of such disclosures.

8. Where the company is regulated by the Financial Services Authority, particular disclosure issues arise. The FSA will expect to be notified about frauds in financial services firms, especially where the frauds have lead to customer losses and where the perpetrators are FSA approved persons.

9. Be cautious when putting observations about the investigation in writing. For example, expressions of doubt about the quality of the evidence obtained may have to be disclosed to the apparent fraudsters and may enable them to defeat a recovery claim. Communications covered by legal professional privilege will be protected from an obligation to disclose but the rules are complicated and legal advice may be required.

10. Be careful when interviewing employees suspected of crimes. The company's (and its insurer's) desire to know the facts must be balanced by the employment law obligations that the company owes to its employees and by the harm it could do to the employee being questioned, without protection being put in place, about matters that might later lead to criminal prosecution.

Steven Francis, partner, and Harriet Boughton, Reynolds Porter Chamberlain LLP

fraud has cost UK companies more than £77m in the first half of 2009, from just £10m for the equivalent period in 2008.

Its research also suggests that employees are responsible for 80 per cent of workplace crime and this upward trend shows no signs of tailing off any time soon.

Some workplace fraud findings make for surprising reading. BDO Stoy Hayward reckons that some 25 per cent of employees has either committed of witnessed workplace fraud, and employers are currently failing to stem the growing tide. Those long-serving employees you have come to know and trust may not be all that loyal; one in four employees committing fraud against their employer has been with the company for more than ten years, which makes the MI5's recent publication on personnel security all the more relevant.

According to the report, many employees who eventually abuse their employment positions did not present significant security risks when they were originally appointed: "Instead, the risk they present increases during the period of their employment".

In an attempt to reduce the risk of the threat from fraud, organisations have begun to manage the risk more proactively, attempting as much as possible to ensure the 'right' individual is hired to begin with, and sometimes even more than that. Rupert Emson, of UK-based pre-employment screening firm, Vero Screening, has worked in the pre-employment industry for some ten years. "One of the areas where we're witnessing changes would relate to the performing of annual checks, or 'ongoing monitoring'."

Measuring good practice is an essential part of the task. Emson points to the Financial Services Authority's (FSA) April 2008 Data Security review which audited around 40 financial services firms to find out what sorts of employment screening checks they were performing with a view to isolating what they would consider to be good practice, as well as commenting on bad practice.

Emson believes this has already had an impact on attitudes towards staff checks. "Traditionally we have not witnessed many firms applying annual checks, although I have to say that this is now changing following the report," he says.

Among the key considerations of the report are the importance of taking a risk-based approach when applying screening levels, ie one-size should not fit all; the importance of certain annual checks on some positions, and the fact that background checks applied to temporary or contract staff should be at a level not less than those applied to permanent hires.

FURTHER INFORMATION

CIFAS, the UK's Fraud Prevention Service recently teamed up with the CIPD and produced a helpful guide *Tackling Staff Fraud and Dishonesty* which dedicates a chapter to vetting and screening, and to monitoring of staff. See www.cifas.org.uk

MI5 *Managing the Risks*' relates to ongoing personnel security management. The current version was updated in December 2006.

WORST CASE SCENARIO – THE INSURANCE PERSPECTIVE

While D&O providers should be expected to thrive in this environment, so too are those offering or broking fidelity or crime insurance. Fidelity insurance covers loss of property due to an employee's dishonesty, as well as suspicious loss of property that cannot be directly attributed to a particular employee. Wordings vary and much will depend on the exclusions that operate but it will generally be in insurers' interests for the perpetrators of fraud to be identified. That way, insurers who pay out under a policy will have a chance of recovering their outlay from the fraudsters directly.

In order to maximise their chances of recovery, insurers, loss adjusters and brokers might have regard to these ten tips:

1. Control very carefully who knows what about the internal investigation. Secrecy may be crucial but is difficult to secure where information is widely disseminated.

2. Consider whether injunctions need to be obtained against those believed to be in receipt of criminal property.

3. Private law injunctions can be expensive to obtain. In certain cases it might be worth contacting the police to see whether they would be willing to obtain injunctions under the Proceeds of Crime legislation.

4. It is important to consider carefully matters of timing. If insufficient investigation is undertaken before an injunction is sought, the fraudsters may be able to defeat the application, but will nonetheless be aware of the interest in them, and may flee the jurisdiction and take with them or hide their assets. If too much time is taken, then the risk of the action becoming known to the fraudsters is increased. Delay may also enable the courts to conclude that the injunction ought to be refused because there is no evidence that the claimant will be disadvantaged prior to a full trial of the issues.

5. In order to maximise the chances of recovery it is important to identify all those who may have aided and abetted the fraud. In a large number of cases, the dishonest employees will have colluded with contractors, customers or suppliers, perhaps benefiting from a kick-back.

6. Be careful where proof of the fraud largely turns on digital evidence. In such a case, consideration should be given to employing an IT forensics expert who can establish to a court's satisfaction that the evidence presented is a faithful record of electronic information contained in a digital device that was properly functioning at all material times.

7. Be aware of the company's obligations to the criminal and regulatory authorities. For example, some types of employee crime may involve the company in the commission of offences, in the underpaying of tax or duty, or to the overcharging of customers. Careful thought will have to be given to whether disclosures should be given to authorities and the timing of such disclosures.

8. Where the company is regulated by the Financial Services Authority, particular disclosure issues arise. The FSA will expect to be notified about frauds in financial services firms, especially where the frauds have lead to customer losses and where the perpetrators are FSA approved persons.

9. Be cautious when putting observations about the investigation in writing. For example, expressions of doubt about the quality of the evidence obtained may have to be disclosed to the apparent fraudsters and may enable them to defeat a recovery claim. Communications covered by legal professional privilege will be protected from an obligation to disclose but the rules are complicated and legal advice may be required.

10. Be careful when interviewing employees suspected of crimes. The company's (and its insurer's) desire to know the facts must be balanced by the employment law obligations that the company owes to its employees and by the harm it could do to the employee being questioned, without protection being put in place, about matters that might later lead to criminal prosecution.

Steven Francis, partner, and Harriet Boughton, Reynolds Porter Chamberlain LLP

fraud has cost UK companies more than £77m in the first half of 2009, from just £10m for the equivalent period in 2008.

Its research also suggests that employees are responsible for 80 per cent of workplace crime and this upward trend shows no signs of tailing off any time soon.

Some workplace fraud findings make for surprising reading. BDO Stoy Hayward reckons that some 25 per cent of employees has either committed of witnessed workplace fraud, and employers are currently failing to stem the growing tide. Those long-serving employees you have come to know and trust may not be all that loyal; one in four employees committing fraud against their employer has been with the company for more than ten years, which makes the MI5's recent publication on personnel security all the more relevant.

According to the report, many employees who eventually abuse their employment positions did not present significant security risks when they were originally appointed: "Instead, the risk they present increases during the period of their employment".

In an attempt to reduce the risk of the threat from fraud, organisations have begun to manage the risk more proactively, attempting as much as possible to ensure the 'right' individual is hired to begin with, and sometimes even more than that. Rupert Emson, of UK-based pre-employment screening firm, Vero Screening, has worked in the pre-employment industry for some ten years. "One of the areas where we're witnessing changes would relate to the performing of annual checks, or 'ongoing monitoring'."

Measuring good practice is an essential part of the task. Emson points to the Financial Services Authority's (FSA) April 2008 Data Security review which audited around 40 financial services firms to find out what sorts of employment screening checks they were performing with a view to isolating what they would consider to be good practice, as well as commenting on bad practice.

Emson believes this has already had an impact on attitudes towards staff checks. "Traditionally we have not witnessed many firms applying annual checks, although I have to say that this is now changing following the report," he says.

Among the key considerations of the report are the importance of taking a risk-based approach when applying screening levels, ie one-size should not fit all; the importance of certain annual checks on some positions, and the fact that background checks applied to temporary or contract staff should be at a level not less than those applied to permanent hires.

FURTHER INFORMATION

CIFAS, the UK's Fraud Prevention Service recently teamed up with the CIPD and produced a helpful guide *Tackling Staff Fraud and Dishonesty* which dedicates a chapter to vetting and screening, and to monitoring of staff. See www.cifas.org.uk

MI5 *Managing the Risks*' relates to ongoing personnel security management. The current version was updated in December 2006.