

When you discover fraud

One of the greatest challenges to international companies today is fraud. Recent high-profile cases illustrate the fact that corruption and corporate malfeasance can bring down even the strongest of companies. Steve Vickers, president and CEO of International Risk writes on the methods of detecting and confronting this insidious malady.



Steve Vickers

CONSEQUENCES OF FRAUD can be devastating, often resulting in severe damage to a company's brand equity, a decline in investor confidence, a loss of market value and severe civil and criminal penalties.

Enron, WorldCom and Tyco became household names, but for all the wrong reasons; now synonymous with rampant corporate greed and fraud. Closer to home, in Hong Kong, numerous scandals at the Bank of China, CAOC in Singapore and many other regional issues clearly

illustrate the severity of the problem.

The probability is that at some point you will discover fraud in your own organisation. The trick is to understand how to identify fraud in the first instance, how to deal with it effectively, to learn from the process and to prevent future problems.

Not surprisingly, much of the corporate corruption and fraud that takes place today is carried out by insiders and senior company employees or directors, often working in collusion with colleagues or outside suppliers and vendors. Their activities can go undetected for months or years because firms have neglected to establish basic fraud prevention and risk mitigation measures. The standard "tick the box" audit committee approach to fraud risk management simply does not work. Matrix management systems exacerbate the problem -facilitating a "pass the buck" attitude and affording corporate fraudsters the opportunity to explore structural gaps in corporate supervision and oversight.

Interestingly, in the last 20 significant frauds handled by International Risk, all of the companies concerned operated a matrix management system.

Enabling factors to fraud include:

- Matrix management systems;
- Going through significant change - business process re-engineering (BPR); a side-effect of which can result in key controls being abandoned;
- Companies failing to perform effective and practical

"due diligence" enquires before transactions;

- Over dependence on low-cost, poor quality "volume personal checks/ screening exercises" - this due to shortsighted cost constraints and naive HR departments;
- Not questioning suspicious transactions;
- Making unusual cash or off-shore payments;
- Use of BVI or other off-shore vehicles, for no apparent reason;
- Internal controls being circumvented, ostensibly for good reasons;
- Inadequate auditing, both internal and external;
- Are your auditors experienced enough in your specific industry;
- Do they have the seniority to challenge your senior-level staff?

Detection of Fraud -The Hard Reality

There are a number of ways in which fraud is generally discovered. In some cases, customers complain about errors in statements. Other records are found to have been re-written, allegedly for the purposes of neatness.

However, the most common way fraud is discovered is through the ubiquitous anonymous letter or email addressed to senior management.

It is highly unusual for fraud to be detected by internal or external audit - because the numbers always add up!

Effective response to fraud by management

When an organisation has received an anonymous allegation of fraud by letter or e-mail, there are essentially three courses of action open:

- The first is to shred the letter or to just ignore it, I would not recommend this but many companies do just that.
- The second potential course of action is to file it with all the other letters but to do nothing about it. Again, not recommended but slightly preferable!
- Finally, the third option is to verify whether or not the allegations are true and to take immediate or appropriate action.

It is important to keep knowledge of the complaint confidential and to prevent sensitive information from circulating around the workplace. Key concerns and questions which management needs to address include the following:





proceed with criminal prosecutions, a very few will be sympathetic in supporting a business to recover assets, at least in the short term. If a corporation does decide to launch an asset searching exercise, this must commence as soon as possible. The project should be led by senior investigators, up until the point that clear information exists as to the location of assets. At this point, a law firm, capable of working within a multi-disciplinary team should be employed. If several jurisdictions are involved in the case, an international law firm is preferable. However, ensure that the firm concerned is "IT savvy" and understands the use of computer forensics and other modern investigative tools.

When pursuing assets, it is critically important to think of the issue through the eyes of the culprits. Development of a chronology of events, commencing well before the apparent incident is generally a very worthwhile exercise. Many frauds start or are planned far in advance of the actual event and evidence, "footprints in the sand", can often be found by searching months before an incident.

Learning from the incident and preventing fraud in the future

It is important that management, at all levels of the company, understand those areas where fraud can occur and that proactive measures are taken to mitigate against such risks. Equally important, is that managers need to be held accountable for fraud risk management. Employees need to understand how and where to make suggestions and to have the confidence that their complaints will actually reach senior management. Some companies operate "whistle-blower" programmes, where employees can make reports of fraud and corruption to a confidential number.

It is also important to remember that fraud risk management is a continuous process. This process should evolve as the company also grows and changes. Risks associated with new IT systems (perhaps not fully understood by senior management), should not be underestimated nor should implementation of such change be left in the hands of the IT department alone.

Essential business controls

In the final analysis, there are actually only five essential business controls to effectively reduce fraud and corruption. They are:

- Honest employees - but how do we know they are honest and that they will stay honest?
- Strong internal controls - but what if these are not relevant to the local market place such as when US or British systems are "bolted on" into the PRC operations, they fail to pay regard to the vital legal status of chops which simply do not exist in western environments.
 - Strong and visible deterrents - in Asia, we describe this as "killing the chicken in front of the monkey", or maintaining a "zero-tolerance" policy for fraud and corruption.
 - Clear management responsibility - holding managers directly and personally responsible for overseeing fraud risk management.
 - Clear reporting lines - ensuring that matrix management systems do not facilitate or enable fraudsters to explore gaps in reporting lines and responsibility for fraud risk management.

- The actual dollar impact to the bottom line.
- Is the loss covered by insurance?
- Can management otherwise recover losses?
- Who is involved - management, staff, vendors, advisors?
- How was it done and how can we stop further losses?
- Is there a requirement to report to regulators?
- Should we keep the incident from the media because of the impact on our corporate image? (Crisis communication planning)
- Should a report be made to the police?

Major fraud is better investigated along the lines that would be adopted by a corporate "crisis management" team. Senior management need to quickly evaluate the complaint and the likelihood of it being true. Appropriate resources with sufficient seniority, need to be appointed with clear terms of reference, reporting deadlines and the distribution of confidential reports. Complicated cases are much better handled by professional investigators from outside of the victimised company.

Other considerations which need to be evaluated, early in the incident include the actual public relations damage to the corporation and the likely reaction of local regulators, once the case becomes public knowledge. It is important that senior management are kept fully informed but is not directly conducting the investigation and considers how it intends the business to operate in the future, i.e. they should look through the incident to recovery.

A clear decision will need to be made as to whether or not a report should be made to the local authorities if a serious offence is disclosed. It is usually appropriate to take action, both criminal and civil against errant employees. A "zero-tolerance policy" leaves potential offenders with no doubt as to the consequences of involvement in fraud or corruption. However, in certain emerging countries, with less developed legal systems there is a danger of collusion and corruption affecting the issue. Again, it is appropriate to make use of senior investigative resources who know both how to correctly package evidential complaints as well as how to deliver them to the most appropriate quarter; this to ensure that action is actually taken on the complaint.

Recovering assets in emergency situations

Whilst in most countries, local law enforcement (if suitably briefed) can be relied upon to



Contact Steve Vickers at 3120-8688 or e-mail steve.vickers@intl-risk.com