Now part of Financial Crime & Compliance on i-law.com

Fraud Intelligence

For the prevention, detection and control of fraud in all its guises

The stable door is still open!

*We know from experience, write **Nigel Iyer** and **Veronica Morino**, that the true annual cost of fraud is enormous but mostly hidden, at least until the damage is done. Fraud threatens organisations, even whole economies – witness the current global financial crisis, which kicked off with the disclosure of massive mortgage fraud in the US. However, if most is not visible, we ought to ask the question: 'Why do we spend such a disproportionate amount of time, money and effort on investigating after the event rather than on detection and prevention before the worst happens?' This article explores more efficient and alternative approaches to managing fraud risk.*

When news of a serious fraud breaks, it tends to be treated like a mini-crisis; the saying "there's no point shutting the stable door after the horse has bolted" summarises the mood. However, often the most important actions and messages should be about managing morale, the company culture and preventing further fallout. Pursuing one investigation to the detriment of everything else may be likened to all the grooms chasing after the one horse which has bolted, while ignoring the welfare of 99 others still in their stalls... and forgetting to shut the stable door!

Large complex investigations is how many fraud professionals, including litigation departments in major law firms, forensic teams in the large accounting practices and specialist investigators, make a living. Many of these same professionals are also eager to advise their clients on prevention, but it is harder to sell. The market is skewed in favour of investigations, so it is understandable that many experts in the field spend little time on prevention. Perhaps it's time to change the focus.

An answer

Over the years we have taken part in and seen hundreds of investigations into suspected fraud and corruption as well as encountering quite a number of different investigative approaches. Many of these methodologies and practices were structured and thorough, although more than a few were unstructured

Case study – isolation cure

It was clear to all that the supplier of marketing services had overbilled for years to the tune of hundreds of millions of Euros. The list of red flags was long: the supplier had only one customer, and seemed to charge at will, the invoices were vague and obviously inflated, some of the mark-ups applied were outrageous, other well-qualified competitors were not allowed to tender and the procurement department was bypassed. The supplier had effectively become an internal department with a virtual 'licence to print money'. All the signs pointed to insiders receiving kickbacks. The big question was whether an investigation would be worthwhile.

The pragmatic CEO decided that a long, drawn out investigation would be painful and would probably not achieve the desired result. Also he was sure that there were several other similar examples. His simple and effective solution was to empower and encourage the professional procurement department to do its job. Procurement gladly complied; the contract was re-tendered, which resulted in annual costs being halved. Nearly everyone agreed that the quality of service improved dramatically. The fraudulent supplier soon went out of business. News of this action, and that the company was no longer a soft target, spread throughout the supplier community rapidly and haphazard. Almost without exception, fraud investigations are complex and costly exercises, which tend to overshadow the more proactive solutions that can keep fraud at bay. It is easy to understand that the return from investing in raising awareness or in an effective detection programme is likely to be tens, possibly hundreds of times higher than for a large investigation. We should never wait for a fraud to happen. [1] Unfortunately executives sometimes fixate on the investigation and lose sight of other actions they should have taken. It's easier to throw money at the visible problems.

The solutions are quite simple but this is possibly also one of the reasons why they are so easily blindsided by "a big case". Here are five simple rules of thumb that we suggest executives should follow:

- the fraud management budget should be spent on areas where there is going to be the best return on investment, ie, predicting where fraud will happen and pre-empting it. This means stopping the criminals from committing the big frauds;
- raise awareness by motivating people in the organisation to discuss fraud risk and training them to recognise the early warning signs of fraud and excessive greed;
- avoid impulsive reactions when confronted with the signs of fraud. Instead carefully consider all options;
- an investigation should be conducted in incremental steps under tight management control and always working to set objectives;
- Even while performing the investigation it is important to work in parallel to identify root causes of what went wrong and look for opportunities to improve the culture in the organisation.

Happening all the time...

Figures like 5% of turnover are gradually being accepted as the true annual cost of fraud and corruption: calling fraud a "risk", therefore, when it is in fact a certainty, is misleading.

Greed, a major driver behind fraud, is just another aspect of human nature. So, rather than being

Case study – investigation is a rocky road that often twists and means compromise

Some years previously a routine Heath Check (a review designed to pick up the red flags of fraud) had identified that a country manager had granted a large services contract to a supplier, which appeared to be controlled by some former associates and possibly the country manager's wife. This information was reported to the regional manager who referred the matter to the legal department, which, after some months, reported back that there was no conflict of interest because dealings with that supplier had been approved prior to the country manager's recruitment.

Two and a half years later a financial controller reported that the same country manager and his associates were colluding with customers and falsifying figures. However, the new regional manager was too busy to review the information and both the fraud risk manager and corporate security had too many other pressing priorities to address the concerns.

Finally, one year on, an anonymous group of people within the company wrote to head office alleging that the country manager had set up a parallel company and was encouraging customers to transfer their business while at the same time submitting vastly inflated sales figures to the head office. This time the regional manager did react. He wanted the investigation to be given top priority. In just a few weeks, conclusive proof of the falsification of figures was established. A plan was agreed to suspend the country manager pending a full investigation.

Just three days before the planned suspension, the regional manager foolishly decided (he felt it was within his remit) to speak personally to his country manager about some of the allegations. Within hours of the conversation most of the evidence was removed and destroyed. The costs of the fraud and subsequent investigation multiplied ten-fold each time the red flags were ignored or a mistake was made.

In the end people in head office took a pragmatic view. Too many mistakes had been made along the way to give a thorough investigation any real chance of success. The ultimate goal had to be the future stability of the company. It was decided to swallow the losses, focus only on the wrongdoings of the most senior manager (who was dismissed) but make it known in the whole organisation what steps had been taken. Luckily this strategy seemed to work. The "good" people in the organisation, who had been prevented from speaking up, saw this as the signal to do so. The people who supported the former managing director either quietly left or (hopefully) changed their ways and the business slowly recovered.

Case study - zero tolerance or just tolerance?

The management team met in emergency session to discuss false expense claims submitted by the absent marketing director. Several directors called for his immediate dismissal and for criminal and civil action The chief executive listened to all the arguments and agreed that the marketing director should be punished. He then asked the directors present to vote on what form the penalty should take, adding one note of caution: "You should vote to extend the investigation, and for prosecution and dismissal if you are absolutely sure that you have not, at any time, done anything similar with your own expenses, and you have not breached the company's code of conduct during your own employment. After what has happened, I am determined to leave no stone unturned."

Rather surprisingly (or not, as the case may be) nobody voted for dismissal and prosecution. It was time to think again about the merits and consistent application of the company's "zero tolerance" policy.

surprised whenever fraud and corruption surfaces, we should start accepting that they are normal behaviour for certain individuals and plan accordingly.

Greed and naivety are closely related. Bernard Madoff needed thousands of naive – some greedy – investors for his monumental scam to succeed. [2] Four remote Norwegian municipalities (total population under 50,000) purchased US$120 million of sub-prime mortgage debt imagining that it had the same creditworthiness as a government bond. [3] The collapse of the Icelandic economy has been attributed to the actions of just a few based in greed and fraud. [4] Maybe investors placed too much faith in the country's rating in Transparency International's Corruption Perceptions Index, from which they understood that Iceland was fraud and corruption free. Whatever the explanation, everybody missed the glaring warning signs.

The cost-benefit equation

Whether we are talking fraud in a company or a corruption 'pandemic', we can be confident on one point, the investigation will take time, tie up resource and probably cost a lot. On the positive side, an investigation can prove cathartic and serve to deter other potential fraudsters. Most executives we have met at the outset of their first big investigation lean towards prosecution until they realise the poor cost-benefit ratio. Protracted, expensive inquiries wear down executive determination.

Even when recovery efforts are successful, to the cost of the investigation often exceeds the original loss, especially when asset tracing fees in relation to monies held offshore and through front companies are taken into account. It is also worth reflecting on the cost to the taxpayer of investigating every Member of Parliament, suspected of misusing their expenses.

Lessons

It's time for a radical rethink about how executives approach the wave of fraud we are seeing. For the past ten years or so 'zero tolerance' has been much in vogue. Many organisations, inspired by zero tolerance policing, which claimed success in reducing the numbers of violent assaults on the streets, adopted a similar policy towards financial crime and ethics breaches. Unfortunately, zero tolerance in this context is often applied selectively. Organisations that ruthlessly punish infractions at the lower levels may fail to apply the same standard to more senior perpetrators. It's easy to punish the small guys, the big fish are much harder to land, and are more likely to fight back. As we have seen over the years, coming down hard on petty financial fraud can distract us and leave the much bigger fraudsters in place.

Opening our eyes

Before launching headlong into an investigation, or become dizzy at the thought, executives need to think about their other options.

Every investigation should comprise two components: one, determination of what went wrong and who got away with it and two, why they went wrong and who and what allowed it. When dealing with faults in a manufacturing process, management has for many years understood that the second component is more important. Unfortunately, this realisation is less widespread when it comes to addressing fraud 'defects'. In the rush to 'get it over with', identifying and addressing the root causes is often neglected.

Companies are often already at work on many of the solutions but unfortunately these are pushed down the pecking order whenever an investigation is on (which is most of the time in many large and medium sized organizations). Following on the rules of thumb given above there are some simple guidelines, which we believe can make life easier and break the continuous cycle of investigations. The key is to learn to Predict, Pre-empt and Prevent fraud and corruption. There are some straightforward ways to do this:

- management and staff should participate in simple 'think like a thief' exercises in order to start looking at the company from a fraudster's perspective. This is the basis of profiling by which the company identifies its major fraud exposures;
- techniques should be developed to detect red flags early. [5] This might lead to a number of 'micro' investigations but these are very easy to manage;
- discretion is a cornerstone of any investigation steps should also be taken before, during and afterwards to make people more aware of the threats of fraud, corruption and unethical business behaviour. Prepared and alert employees are an invaluable resource in helping make companies resistant and resilient. Sending a message across the organisation (by de-heading the snake, as discussed in the second case study) may be just what is needed.

Several years ago, senior management in one organisation informed said, "We want to give you our full support for the excellent work you are doing with internal controls to prevent fraud, and also the investigations you have carried out. However we are not so sure about this proposal of yours to detect lots of fraud. I mean what are we going to do with all the frauds you find... investigate them all?"

Thankfully, our clients today are much more proactive, support the use of fraud detection techniques and accept the temporary increase in the number of fraud investigations but not necessarily the size of them. We believe it is the way of the future.

Notes

1. "A new approach for a new era" by Jim Gee, *Fraud Intelligence* August/September 2009
2. "All just one big lie" by Timon Molloy, *Fraud Intelligence* February/March 2009
3. See note 1 above.
4. "Revising a Definition of Corruption as a Result of the Global Economic Crisis - The Case of Iceland, in Organizational Immunity to Corruption: Building Theoretical and Research Foundations," Vaiman, V., Davidsson, P.A., & Sigurjonsson, T.O., Warsaw: Polish Academy of Sciences.
5. "Pre-emptive strike" by Richard Minogue and Nigel Iyer, *Fraud Intelligence* April/ May 2009

Nigel Iyer *(nigel.iyer@septiagroup.com) originally trained as a Chartered Accountant but has worked in the prevention, detection and investigation of fraud and corruption for over 20 years. He is the author of "Fraud and Corruption Prevention and Detection" and the management novel "The Tightrope". Today he writes drama and screenplays about the human effects of corruption and holds a Masters Degree in Screenwriting. His latest book, "A Short Guide to Fraud Risk" for CIMA and published by Gower, will be out in early 2010. Only one chapter out of seven is about investigations.*

Veronica Morino *(veronica.morino@septiagroup.com) has over the past ten years applied her academic training in sociology and science of the organisation to the field of fraud and corruption, first investigating many frauds and then focusing on prevention; she is working on measuring the resistance and resilience of organisations to fraud and corruption. Her book, "The Anatomy of Fraud and Corruption" (Morino, Minogue and Brytting) will be published in 2010.*

Editor: Timon Molloy • Tel: 020 7017 4214 • Fax: 020 7436 8387 • Email: timon.molloy@informa.com

Production Editor: Frida Fischer • Tel: 020 7017 5501 • Email: frida.fischer@informa.com
Publisher: Victoria Ophield
Sales and renewals: Pauline Seymour • Tel: +44 (0) 20 7017 5063 • Email: pauline.seymour@informa.com
Subscription orders and back issues: Please contact us on 020 7017 5532 or fax 020 7017 4781.
For further information on other finance titles produced by Informa Professional, please phone 020 7017 4108.
Printed by: Premier Print Group • This newsletter is printed on paper sourced from sustainable forests.
ISSN 0953-9239 © 2009 Informa UK Ltd
Published 6 times a year by Informa Professional, Telephone House, 69-77 Paul Street, London EC2A 4LQ. Tel 020 7017 4600. Fax 020 7017 4601. www.informa.com

informa
law
an **informa** business

Informa UK Ltd, Registered Office: Mortimer House, 37/41 Mortimer Street, London, W1T 3JH.
Registered in England and Wales No 1072954.