www.informaprofessional.com/fi

Fraud Intelligence

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

Something rotten discussed in Denmark

A three-day Fraud & Corruption Summit, the fifth, held annually in Europe by MIS Training Institute, recently brought together speakers and participants from Denmark, Europe and beyond. ***Esther Martin*** *reports.*

For hundreds of years the tale of Hamlet's tumultuous spiral to destruction because of his uncle's treachery has been hissed from stages around the world. Given Denmark's current top-equal ranking in Transparency International's Corruption Perceptions Index, this seems like rather unfair branding on Shakespeare's part. However, the country became the hub of discussion of dastardly deeds again recently – how to detect, investigate and prevent them, that is – when the harbour capital of Copenhagen hosted a Fraud & Corruption Summit. Notes from a few of the sessions are presented below.

The resolute investigator

"There's something about being obsessive about things, which makes us good at what we do," said Peter Tickner, who has headed internal audit departments at both HM Treasury and the London Metropolitan Police. For some, this might not seem the most flattering of compliments, but Tickner's approach is all about being single-minded. "Begin with the end in mind" is his mantra.

"Fraud is much easier to prove than corruption and you're much more likely to get your money back," said Tickner. He argued that staff time spent on fighting fraud is a good investment as "Fraud investigators can bring money in when times are hard." But in tough economic periods, he said, organisations needed to rely more on in-house professionals and existing skills in internal audit and cut back on use of expensive 'big four' forensic services. There are plenty of smaller specialist players available, he noted.

Sources for finding the fraudulent and corrupt might include referrals from the Human Resources department; reports or requests for help from line managers; informants and anonymous tip-offs; analytical review of business systems; routine audits; fraud awareness training and seminars; internal and external whistleblowing; and – in the UK – the National Fraud Initiative, he said.

Tickner suggested targeting areas of greatest fraud risk and using simple techniques like Benford's law – which analyses the standard pattern of occurrence of digits within datasets. "If you know what the normal profile is for your organisation, you can tell if someone's ripping you off," he said. If goods have standard prices like €99.99 that will skew results, but you can see "if any individuals have very different profiles".

If a fraud is identified, Tickner said the first step is to hold an initial planning meeting. Key players to be present include the chief investigator or chief internal auditor, the person who will lead the initial investigation, the internal legal adviser, someone from Human Resources, and a senior executive who isn't the chief executive or equivalent. Regarding the absence of the CEO, Tickner explained that "If the investigation goes wrong the chief executive will need to oversee any internal disciplinary process and they will have their hands tied if they were actively involved in directing the investigation." He added: "If it is a senior employee committing the fraud and they appeal against any action taken as a result of a successful investigation then the chief executive will be in a position to arbitrate without falling foul of employment law." The person reporting or making the allegation of fraud should also attend, to explain in their own words. "After that they may be excluded if they are potentially too close to the action. If, on the other hand, the source is an auditor or investigator who has found the evidence then you may well keep them there," explained Tickner.

It is vital to establish the basis of the investigation and sort out the protocols, he said: "If the organisation has a fraud response plan, are you following it? If not, who will do what? But don't forget the need to take urgent action if the fraud is still ongoing." The terms of reference for

the investigation should be agreed by senior management, signed and kept safe, advised Tickner.

The key to managing an investigation and making effective decisions is to begin with the end in mind, said Tickner: "The art of a good investigator is to home in on the most serious and easy to prove things and go for them." He suggested these priorities when a fraud is found: first, to stop it, then recover what can be recovered, fix any system weaknesses, and finally to pursue and punish the guilty.

"Criminality can wait. That can come last. Once you've reported someone formally to the police that limits what you can do," he said, "Don't let outside people run your investigation. You can do things the police can't. If someone confesses, it's allowable evidence, whereas, police have to caution them first. Those who know police rules would have to do the same."

Tickner's approach is to investigate for facts, and not rules. "Do not give your investigation to a lawyer … I want to find out the facts and when I get the facts I'll decide if the law matters or not," he said, "When you've got them, then you know what the problem is. Then you might talk to your lawyer."

He differentiates between intelligence and evidence: "I'd much rather have the intelligence even if I can't use it as evidence – at least I know I've got the right person. Get the intelligence right, get the end in mind and then work out what you're doing with it." As an aside, he noted that not everyone is aware that "it is legal to tape telephone conversations provided you're a party to the conversation". He also suggested, "If you get a chance to take out a freezing order I would always go for it." It's a "psychological thing".

Once you know what you've found, Tickner said the investigator should prepare an interim report for management, consisting of a "short, sharp summary with limited supporting evidence and clear recommendations for the next steps." At the end of the investigation, produce the full report, the final record, with all relevant documentation and evidence, he said.

Bank fraud case study

"There's an awful moment when you realise it must have been instigated by someone inside – one of your colleagues," said Sean Holohan, director for financial crime and anti-fraud audit team leader at Barclays in London, of his experience of investigating frauds at the bank. Internal staff collusion is management's worst nightmare, he said. "Organised criminals attack banks in a very coordinated way."

"Password sharing is rife and we need to stop and stamp it out. Even a strict line where people are dismissed for sharing passwords hasn't stopped it," he added.

Holohan shared a case study of a fraud the bank experienced outside the UK. It involved a branch manager acting in collusion with a third party, who overrode new account-opening controls to open an account in the name of a third party. To do so, the manager asked a more junior assistant to stand aside and provided inadequate identification and verification evidence.

The manager was also able to utilise systems access from a previous role in the payments department that had not been rescinded. Along with a colleague in the payments team, they forged payment instructions from a relationship manager – the branch manager acting as one authoriser and the colleague forging the signature of the other authoriser. Transfers totalling several millions were made from innocent customer accounts into the newly opened account – domestic transfers were deliberately chosen in order to avoid the more rigorous controls for cross-border payments. Almost immediately, the funds were transferred to accounts at other banks.

Unfortunately, the bank's whistleblowing systems were not strong in this particular country. Barclays was alerted when customers complained about the unauthorised payments from their accounts. The relationship managers for these customers responded quickly in notifying the in-country financial crime team. The investigators contacted the other banks at once and were lucky enough to recover or freeze around 90% of the funds.

Apart from this, the investigation team was not sufficiently effective however. They discovered the forged instructions but rather than pinpointing key suspects, they identified 13 staff members who could have been involved, all of whom were placed on suspension for three months. The investigators didn't focus on failed controls or look at the account opening process and were unable to determine in any more detail than staff collusion how the fraud had been possible. Their interview skills were lacking, they took too long, didn't establish clear objectives or engage with the legal department. Instead the investigation team liaised with local police, whose enquiries were also inconclusive.

After a request from management, a new independent team of investigators reviewed the evidence. They focussed on the control environment

and how this sort of incident could be prevented. They identified 13 controls that had failed, allowing the collaborators to carry out the fraud. Eleven of the staff were cleared of involvement and brought back to work, and a control remediation action plan was put in place.

Holohan said that areas which had to be addressed within the control environment were absence of 'tone at the top' messaging about appropriate standards; the inadequate monitoring by management of control effectiveness; a lack of understanding about why certain controls were undertaken along with a 'tick box' mentality; and a need for scenario-based testing of 'What could go wrong?'

The bank applied lessons from the experience on both local and regional basis, which meant enhanced controls monitoring; review of all 'maker-checker' controls; refresher training for control operators; reminders about whistleblowing; regular 'tone at the top' messaging; additional training for investigators (including on interviewing and controls); and addressing the willingness of management to admit there is a risk and ask for help so that they can benefit from expertise within the wider group.

In a second case study that involved systematic fraudulent third-party payments made by a trusted, senior financial controller of long-standing, Holohan said the lessons were that reliance on an individual is not a control; healthy scepticism and prompt action are essential; and there should be no exceptions to investigation policies and procedures.

Fighting fraud in Russia, steppe by steppe

If fraud seriously dents profits in the most mature economies, then spare a thought for Russia. Sergey Martynov, chief audit executive at the Siberian Coal Energy Company, said that losses from fraud and commercial corruption in big Russian companies boost production expenses by at least 20%.

The country's communist history embedded fertile ground for fraud and corruption, with characteristics like a traditional lack of respect for private property, tolerance of fraud, flawed and poorly implemented legislation, along with low salaries and an underdeveloped social protection system.

Fraud is built into the system. For instance, Martynov told how siphoning off company fuel to sell on the black market for additional income was accepted practice: "People were not interested in measuring it. A control system was brought in and the drivers went on strike. They felt deprived of their rightful income."

Tolerating this practice actually works out cheaper for companies as it allows them to pay very low salaries, which employees top-up by helping themselves where they can. "A company prefers to have overrated fuel expenses and low salary. If a company pays salary it additionally pays social tax," he explained. "[And] if you pay taxes you have no funds of dirty money for corruption.

"In Russia the social security system is so weak that no one considers it seriously. Everyone has to take his own profit in an illegal way," he said.

Tax evasion has been rife in Russia since it embraced capitalism but, assisted by a successful low flat tax brought in a decade ago, the government's take has been improving. As the tax capture has grown, companies have less money to cover staff fraud and are having to take measures to prevent it. The government is also acting to support private companies in preventing fraud and corruption.

"For big Russian companies this is a process of raising salaries. It's impossible to do it in one day," said Martynov, "If you do it in one day you will receive a strike."

Siberian Coal Energy Company has installed fuel metres to measure consumption and its greatest vulnerability to fraud is now in the area of management accounting. In the transition from a regime where "there was a Ministry of everything you can imagine" to private enterprise, "every company decided for itself how to manage the system of management accounting or whether to have it at all" said Martynov, "Clever people realised they had an endless supply of funds."

As part of a counter fraud programme, control procedures have been introduced and detection and investigation activities are undertaken. A hotline, which can be used anonymously, has been set up. "We receive ten calls per week on our system, which is a very good result," said Martynov. Polygraphs are considered a "normal process" when conducting counter fraud work in Russia.

The strategy also involves working with senior managers so they understand the seriousness of their fraud and corruption threats, and developing a corporate culture of honesty and aversion to fraud. "Changing the culture of a company to be anti-fraud is a process of some years and you have to do it step by step," said Martynov.

www.i-law.com/financialcrime

Editor: Timon Molloy • Tel: 020 7017 4214 • Fax: 020 7436 8387 • timon.molloy@informa.com
Editorial board: John Baker – Director, Risk Management – Fraud Solutions, RSM Tenon • Neil Blundell – Head of Fraud Group, Eversheds • Andrew Durant – Senior Managing Director, FTI Forensic Accounting • Chris Osborne – Director, Dispute Analysis and Forensics, Alvarez & Marsal
Production: Catherine Quist, tel 020 7017 6242 • catherine.quist@informa.com **Printed by**: Premier Print Group, London
Sales and renewals: Leyla Utman • Tel: +44 (0)20 7017 4192 • leyla.utman@informa.com ISSN 0953-9239 © Informa UK Ltd 2010
Subscription orders and back issues: Please contact us on 020 7017 5532 or fax 020 7017 4781. For back issues or further information on other finance titles produced by informa Law, please phone 020 7017 5532, or fax 020 7017 4108
Published 6 times a year by: Informa Professional, 1/2 Bolt Court, London EC4A 3DQ • tel 020 7017 4600 • fax 020 7017 4601. www.informaprofessional.com

informa
law & finance
an informa business