

FEATURE ARTICLE

As experts predict an increase in internal crime due to the worldwide financial recession, this article investigates how in-house counsel can work with their colleagues to prevent and contain this risk.



The risk within: white collar crime

International risk consulting company Kroll International has recently released its Global Fraud Report. Recalling the increase in white collar crime that occurred in the dark days of 1987, 1991 and 2001, it predicts that the current worldwide financial recession will result in a similar surge in internal crime. PriceWaterhouseCoopers (PwC), which conducts biennial global economic crime surveys, reports that the trend is already discernible. 'Increases in internal fraud are already apparent,' comments Andrew Gordon, Partner in Forensic Services and Head of Investigations Practice in the United Kingdom. The reasons are clear, he says. 'In good times there's more opportunity for crime – people wave things through and they're not paying close attention. But in bad times, employees are under more pressure to perform and under personal pressures too and can start to rationalise their criminal conduct.'

Rosalind Wright, Chairman of the Fraud Advisory Panel in the United Kingdom, a charity that advises on fraud prevention and management, also believes that the future for internal crime looks bleak. 'Employees who are under pressure, especially when they're under the threat of redundancy or if the company is expected to fail, seem to lose their moral constraints and turn to crime. In some cases, it's pure desperation.'

But if internal malfeasance is on the increase, are companies prepared to deal with it? Probably not. 'People are very complacent

about fraud and don't see it as a business risk,' says Wright. Both Wright and Gordon agree that, paradoxically, just when companies most need to be vigilant, they reduce the controls on internal fraud. 'Now organisations are cutting back on people like internal auditors because they don't contribute to the bottom line. This is very worrying,' notes Wright. For in-house counsel, the trend is likely to result in their involvement in more internal investigations, regulatory interference and legal wrangles. So how can in-house counsel work with their colleagues to prevent and contain internal crime?

Prevention better than cure

For a start, experts insist that standards must be set firmly and at the top to be effective. Helen Mahy, Group Company Secretary and General Counsel of National Grid plc, who is also responsible for Group Risk and Compliance says: 'The key thing is your corporate culture. You have to have clear business and ethical codes that you reinforce constantly so people know what behaviour is unacceptable and what is expected of them.' While fraud needs to be constantly on the agenda and at the forefront of the minds of top management, legal teams are often charged to work with compliance, finance and audit teams to shape and implement anti-fraud policies.

They confront a range of potential threats. As well as employees who are unhappy and

Diana Bentley is a former practicing lawyer and is now a journalist, writer and public relations adviser based in London. She can be contacted by e-mail at dianab@dircon.co.uk

under pressure, companies are at risk from employees who are naturally opportunistic too. 'Employees can also be placed in organisations specifically to get confidential information,' warns Toyin Adedokun, Senior Consultant at SunGard Availability Services, a UK business continuity and disaster recovery specialist. Classic examples of what employees can get up to he says, include claiming unjustified overtime and sick leave, falsifying work and income, collaborating fraudulently with suppliers, stealing company assets and deliberately interfering with company property like trade secrets and IT systems.

But sound in-house practices, that begin before employees arrive and end after they have left, can effectively contain crime. At the outset, rigorous re-employment screening is advisable. Forensic specialists like PwC report that around one in four CVs is exaggerated and one in ten contains lies about qualifications or experience. Employment contracts and confidentiality agreements are good weapons against internal misdeeds and contain stipulations like forbidding the later use of company information and poaching clients. 'These agreements can be relied on later if breaches occur,' says Nicholas Lakeland, an Employment Law Partner of London city firm, Silverman Sherliker. 'Employment contracts should also contain protective devices like enabling the employer to look at personal e-mails and business e-mails which help ward off invasion of privacy claims.'

Informing and educating staff about the threats of internal fraud is crucial experts say, and introducing anti-fraud policies should be part of the initiation process for all employees including temporaries. Anti-fraud policies however, may not always come labelled as such, says Lakeland. 'Often these policies are part of good conduct policies, policies on conflicts of interest and the company's intellectual property rules which may be contained in company handbooks and the like.' These written policies, which in-house counsel often help draft, not only reinforce general behavioral standards, but inform employees on how to follow them in practice and make them aware of the penalties involved for breaches.

Anti-fraud policies should be embedded in daily management activities but can be easy to implement, insists Andrew Gordon.

'Companies often have online educational programmes. Employees can undertake a programme, do a questionnaire then sign an acknowledgment that they've read and understood the policies. Companies should do this annually.' At National Grid, General Counsel Helen Mahy is responsible for the group e-learning and team talks that address the organisation's standards of ethical business conduct, competition matters and licence compliance.

Whistleblowing policies that encourage employees to speak up are essential in ensuring that employees have specific, trained staff to go to and to know how they can be protected. Helen Mahy's department in National Grid establishes the group's whistleblowing schemes to ensure that they comply with legislation and best practice in the area. 'Normally it's best practice to not only have someone within the organisation for employees to talk to but someone outside as well,' advises Mahy. While many complaints to hotlines focus on harassment or discrimination matters, cases of fraud can also be disclosed.

IT system security is also crucial. 'Companies should ensure that their data is effectively backed up. Should someone be able to breach your security and take down or sabotage your IT system, it's essential that you be able to recover all your data and information as quickly as possible,' says Toyin Adedokun. 'And you need a business continuity plan – something that states what you'll do if you're unable to access your building or your critical IT systems and processes. The plan should be realistic and workable, communicated to all of your staff and tested at least once a year.'

Other practical rules aid the fight against fraud. 'Companies should constantly monitor inventories and invoices,' adds Adedokun. 'We advise people who run call centres to ban all paper, pens and printers in the centres which would enable employees to take information away with them.' Segregating duties is a basic method of combating crime, and one that should remain at all times, says Andrew Gordon. 'Normally in back offices, one person authorises an expense and another signs off on it. In bad times, staff can be cut back and one person performs both functions. Routine controls like this can go. But internal audit is an essential deterrent in the fight against crime. If that function is reduced, people will be bolder.'

Companies can also take precautions like monitoring employees who habitually arrive early and leave late and who don't take leave, says Nicholas Lakeland. 'Employers should insist that employees take their leave. This is often when fraudulent behaviour is uncovered.' And when people leave the organisation, companies must ensure that their access codes to all systems are immediately disabled and common passwords changed.

Such attitudes reinforce the standards that boards and senior management set. 'It's a part of the tone that should be set at the top,' agrees PwC's Andrew Gordon. 'CEOs, boards and senior management must devote time to the subject and say "we don't allow fraud or any other crime here" and come down very heavily on those who are guilty of it.' ❖

How to deal with breaches

While companies need to be clear about who will deal with internal malfeasance, in-house counsel will often find themselves involved before and after detection, with evidence gathering and dealing with police. When companies become suspicious of employees, care needs to be taken in establishing guilt and gathering evidence. 'Quite a lot of thought is required,' says Nicholas Lakeland. 'It often pays to call in experts. What advice you can get naturally depends on what you can afford. But if you don't get skilled people, they mightn't understand the game that's being played. Good forensic computer people who can deconstruct hard drives are well worth the expense. Getting advice from litigation counsel on evidence gathering is useful too.' Larger organisations may also have staff specifically responsible for enforcement. 'We have trained people in-house who deal with cases of potential fraud and provide specialised advice on them,' says Helen Mahy.

In cases of serious misdeeds, experts note that companies can be dangerously inclined to avoid the negative publicity that can be involved in bringing them to account. 'In some cases, particularly in the financial services industry, you must comply with relevant legislation and matters have to be reported to authorities,' says Rosalind Wright. 'But in many cases, there's no obligation to report the matter and people just want to draw a line under it. Not taking action however, can make other employees despondent or encourage them to break company rules or laws too.'

A policy of zero tolerance is best, say experts. 'People here know that we come down hard on any transgressions of our standards and don't hesitate to take appropriate legal action,' says Helen Mahy at National Grid.