

Fraud Intelligence

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

Are you ready for fraud?

*A manager arrives at work on Monday morning or, worse still, he is contacted over the weekend, with news of a potential fraud. What does he do and what should the organisation already have done to prepare? Will it be able to weather the storm waiting to blow up in the media? **Timon Molloy** looks at fraud crisis management.*

The paradoxical rule of crisis management is “be prepared”. While crises are rare, hopefully one-off events, contingency planning pays, and literally saves, dividends. Absence of preparation is like playing Russian roulette: an empty first chamber in the barrel can offer no comfort when pulling the trigger again. Handled badly, a major fraud can quickly destroy a company’s reputation, both internally and externally, and its business, as Andersen, Enron and now WorldCom know to their cost. “A cool head is required, rather than knee-jerk reactions,” cautions Dan Morrison, a partner at the law firm Mishcon de Reya.

“The key questions to answer,” says Roy Daisley, Director of Carratu International, “are who, who else, how, how long for, why, how much, can we recover it, and, very importantly, where’s the dishonesty?” To enable a cool considered response to these questions is the central aim of the Fraud Response Plan (FRP). As with any disaster recovery programme, its purpose is to maintain continuity. The FRP should, as far as possible, ensure business as usual while the incident is investigated. This means that the plan must provide clear guidance about who is responsible for what and specify exactly what should not, as well as what should, be done; a ham-fisted approach to interviews with suspects and to preserving evidence will jeopardise any criminal prosecution.

The plan should include the organisation’s fraud policy, which might state: all reasonable steps will be taken to deter and prevent fraud, and other criminality; all incidents will be investigated; disciplinary action will be taken against staff when appropriate; civil action

will be taken to recover losses and prosecutions will be pursued. Staff should know this policy and employment contracts should set out clearly what is and is not permitted, for example, the attitude to gifts and corporate hospitality, and the disciplinary procedures and penalties. These dos and don’ts should also feature in staff employment contracts which should also permit the organisation to monitor employee communications and use of the Internet subject to *Data Protection Act 1998* and *Regulation of Investigatory Powers Act 2000* and *Human Rights Act 1998* conditions (legal advice on wording of contract terms is strongly recommended).

The FRP should identify the main contact for reporting fraud as well as the parties who are responsible for managing an investigation. The Fraud Response Team (FRT) will comprise representatives of the internal investigations or security section, internal audit, legal, human resources and local departmental management. These individuals, who may have little to do with each other in the course of their day-to-day activities, should meet to rehearse possible scenarios, including the worst case(s), and how they would respond. The team should be tight-knit since “when the fraud first comes to light, the victim will not properly know the full extent of the wrongdoing or those involved,” notes Mr Morrison. On the basis that much fraud is carried out internally or with the collusion of staff, and managers could well be involved, it is sound policy to outsource the fraud reporting hotline.

The FRT will oversee the investigation, devise a project plan, authorise actions, and set and regularly review objectives, namely criminal prosecution, civil recovery, disciplinary proceedings or no further action. It should always be remembered that the suspect(s) is to be presumed innocent until found otherwise. Strict confidentiality must be observed therefore both to protect the innocent and to avoid alerting the fraudster.

Each part of the FRT will have specific responsibilities. Investigations staff will carry out the fieldwork and advise on external specialist resources, for example, surveillance, IT forensics and independent investigation agency support, which is likely to be essential when enquiries extend overseas. Links with preferred outside professionals, of whatever discipline, should be established before the problems arise since they will then not need to waste precious time at the outset learning their way around the business and management structures. The FRT must set their remit with care to ensure that they do not double up on work undertaken by internal staff.

It is essential that evidence is secured as early as possible. With data stored increasingly on computers, it may well be necessary to image hard disks covertly for analysis; it is almost impossible for a fraudster to erase all trace of data from a computer disk, even by re-formatting. Investigations personnel should also be able to advise on compliance with the requirements of the *Police and Criminal Evidence Act 1984 (PACE)*, in order to avoid compromising any subsequent police enquiry, and also manage any relationship with law enforcement.

Internal audit can provide resource for financial analysis and should be able to recommend forensic accountants. They will be able to brief the audit committee of the board and confirm that the detected weaknesses in internal control have been addressed in accordance with Turnbull risk management provisions.

The legal department will provide its expertise to the FRT and liaise with external advisors. In-house counsel should be able to advise on employment law matters, regulatory obligations and on what it is permissible to say to the media, but it is unlikely that they will be familiar with obtaining search and asset freezing orders at short notice. Reports and communications relating to the fraud should be addressed to counsel in order to gain the cover of professional privilege. Legal should also inform the fidelity insurers.

When it comes to public relations, the FRT must decide who are the audiences it needs to address. "Depending on the seriousness, this will include clients, staff, investors, regulators and the media," says Victor Trocki, Managing Director of Trocki Public Relations Limited. "It is essential," he adds, "to take the initiative when a crisis breaks and tell your own story. Leading from the front gives confidence that the

organisation is the most authoritative source of information concerning what has happened and what is being done." What should the different audiences or 'publics' be told, if anything, and by whom? Whatever the chosen messages to each are, they must be consistent. "Risk of bad coverage will be mitigated if the organisation is able to claim that the fraud was identified by routine controls and that you are in control," says Mr Trocki.

The organisation's spokesperson must be media-trained and all staff should be made aware that queries, from whatever source, should be routed to him or her. Although the spokesperson should be senior this does not necessarily mean the chief executive, especially if he or she is not the most effective communicator. Switching spokesman in the midst of any crisis is strongly discouraged as audiences tend to identify and may even come to sympathise with one individual. A change can suggest confusion in the organisation or internal disagreement and is likely to detract from the message. It is vital that the spokesman never admits liability or indulges in speculation about the cause of the crisis. When talking to the media, it is also prudent to work on the basis that nothing is off the record. At the same time it is essential to be straight with the publics. Special care should be taken with the media since any hint of dissembling and investigative journalists will pursue the matter relentlessly. In the words of Napoleon, "Four hostile newspapers are to be more feared than a thousand bayonets." By the same token, however, media coverage should be monitored constantly and retractions demanded in the case of gross inaccuracies. Victor Trocki emphasises that internal communications are as important as external, "Maintaining morale during a crisis is critical as disenchanted staff members could be a potential source of unauthorised comment, bad news travels faster than good news." The press and media should not, however, be seen as the enemy, "Honest dialogue with them can greatly reduce negative publicity," he says.

A distinction must be drawn between audit and disciplinary investigations. If it is decided to pursue only the disciplinary route then the organisation's own staff may interview the suspects. However, if legal action is entertained then it may be wise to bring in external investigators to conduct interviews in accordance with PACE. Human resources can

advise on the internal code of conduct for staff and whether investigative interviews are likely to prejudice subsequent disciplinary action. Dan Morrison points out that “if an employee is under suspicion, it may be appropriate to keep the person employed, at least for the time being, so as to assist the investigation and avoid the concealment of assets or destruction of evidence.”

With an effective fraud response plan in place the organisation may have greater confidence that it will be able, says Roy Daisley, to “limit damage to the company’s finances and its reputation as a safe haven

for investment, prevent repetition, recover lost assets and deter other fraudsters”. Hope for the best certainly but be prepared for the worst.

Dan Morrison, Partner, Mishcon de Reya: tel +44 (0) 207 440 7124, email dan.morrison@mishcon.co.uk

Roy Daisley, Director, Carratu International: tel +44 (0) 208 643 8000, email royd@carratu.com

Victor Trocki, Director, Trocki Limited: tel +44 (0) 207 420 1911, email trocki@keescott.co.uk

Much of the material for this article was gathered at IIR’s Fraud 2002 conference, which was held in London in June 2002.

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

Production Editor: Lisa McMahon • Tel: 020 7017 5703 • Fax: 020 7436 9478 • Email: lisa.mcmahon@informa.com

Marketing: Michaela Glendinning

Publisher: Kelly Furneaux

Subscription orders and back issues: Please contact us on 01206 772223 or fax 01206 772771.

Printed by Masterprint, Charlton, London

For further information on other finance titles produced by Informa Professional, please phone 020 7553 1523.

ISSN 1462-1401

© Informa UK Ltd

Published 10 times a year by Informa Professional Publishing, Informa House, 30-32 Mortimer Street, London W1W 7RE. Tel 020 7017 4600. Fax 020 7017 4601. <http://www.informa.com>

Copyright While we want you to make the best use of *Fraud Intelligence*, we also need to protect our copyright. We would remind you that copying is illegal. However, please contact us directly should you have any special requirements.

While all reasonable care has been taken in the preparation of this publication, no liability is accepted by the publishers nor by any of the authors of the contents of the publication, for any loss or damage caused to any person relying on any statement or omission in the publication. All rights reserved; no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electrical, mechanical, photocopying, recording, or otherwise without the prior written permission of the publisher.

Informa Professional Publishing is a trading division of Informa UK Ltd. Registered Office: 19 Portland Place, London W1B 1PX.

Registered in England and Wales No 1072954.