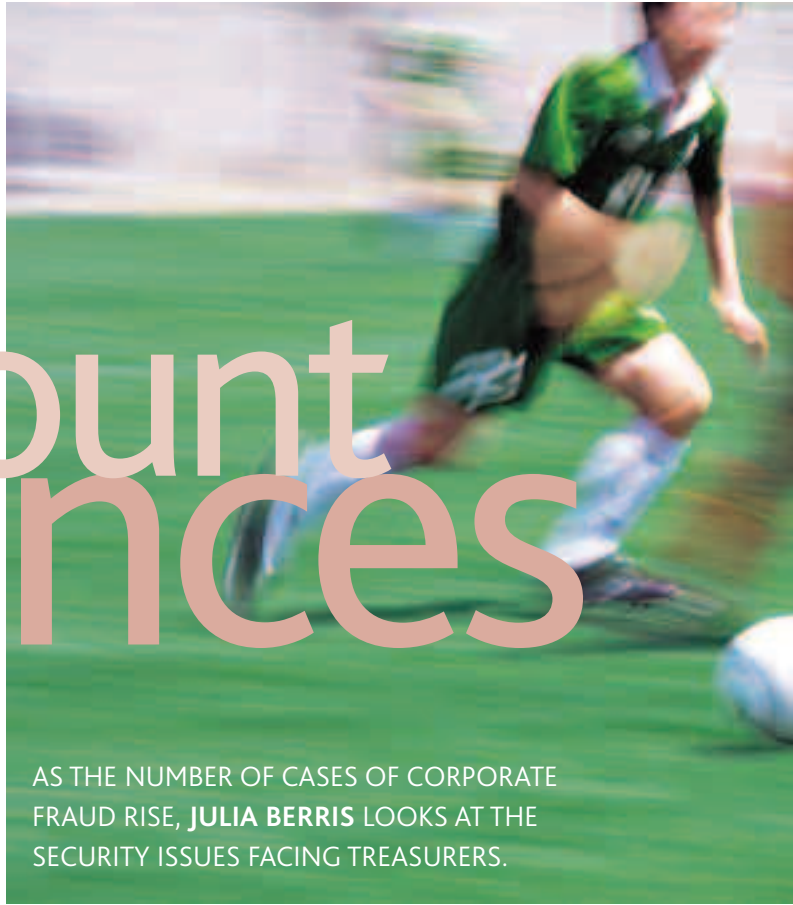## risk management
FRAUD

Mount defences

AS THE NUMBER OF CASES OF CORPORATE FRAUD RISE, **JULIA BERRIS** LOOKS AT THE SECURITY ISSUES FACING TREASURERS.

The Queen's Speech in November 2006 included legislation to simplify fraud trials, tighten up the national strategy on fraud and – controversially – reopen the question of juryless trials for fraudsters. The moves follow the introduction of the Fraud Act, which, for the first time in 150 years, creates an offence of fraud.

The move is timely as it coincides with a big rise in corporate fraud in the UK. According to KPMG Forensic's Fraud Barometer, 2006 saw 277 fraud cases come to court, the largest number ever recorded in the 20-year history of the barometer. Over 40% of all fraud cases in the second half of last year were carried out by professional criminals (63 cases out of 154), compared with a quarter of cases in the first half of the year (30 out of 123). Companies' own managers were responsible for 40% of fraud by value (£350m) – a clear sign that organisations need to protect themselves from this risk and learn how to spot insider activity.

So what are risks associated with fraud and the treasury department and what can the treasurer do to minimise them?

ENTERPRISE-WIDE Promoting awareness in the whole organisation is of the utmost importance, says Dick Price, Senior Information Security Consultant at Beacon IT. "Treasurers need to ask important questions such as, what are the controls that we need and do we currently have them? If not, how can we achieve this security? They need to develop more of an awareness of the various security precautions that need to be taken and to talk to IT people who can really help them implement these measures."

A well-designed and secure treasury management system is a must in a busy treasury department. Too often, even basic security measures are ignored because the level of risk has not been fully understood by senior management.

Price says: "Quite often, there isn't senior management support. They often see it as an IT-only issue. It is much broader than that. Treasurers should be more connected with those who can assist them. Regular discussions with the IT department would help to keep on top of any problems with the security."

Increased awareness via regular meetings with the IT department has to be embedded into the culture of the company. This takes time and would probably require a strategy plan to implement.

On a day-to-day basis some simple things can be done to make it harder for hackers to retrieve vital information from your department. Price says: "A lot of the time fraud has become possible because employees have been bad at remembering the simple rules. It's often very basic, common sense things such as not giving out passwords or personal information over the phone. You also need to think of the basic hardening of systems such as changing default passwords."

Many departments are good at keeping details of passwords within the confines of the treasury team, but it is easy for the security-conscious attitude to slip. When employees move on and new recruits come in, instilling the same level of security awareness is not always easy.

The recruitment process itself can cause difficulties. Pat Leavy, Executive Director at treasury consultancy FTI, says: "When recruiting, the aim is to find someone as soon as possible. This can mean that references are not followed up adequately. Treasury has become very demanding. If you get it wrong when recruiting, there could potentially be significant dangers for the company."

A well-structured and organised treasury department is a benefit in many ways. In terms of protecting your company against fraud, organisation is a must.

Leavy says: "There must be segregation between front, middle and back-office functions. Some treasury departments may not be large enough to physically separate these functions, but segregating the processes – such as execution, confirmation and settlement – is still achievable." This also helps make the auditing process run more smoothly.

Leavy says: "Auditing is clearly very important for a treasury department. My view is that in a lot of cases, the auditing process is not very well developed. You can't just employ a standard auditing process. It has to be detailed and specific to treasury."

As technology and treasury advance, the ability to manipulate systems to obtain information has increased. While straight-through processing (STP) minimises manual processes, removing a large risk for error and misuse of information, not all corporate systems are compatible with banking systems.

Leavy says: "The reality is that STP is quite a challenge. There are so many different electronic banking systems out there and it can be hard to ensure proper interface between a treasury management system and the bank."

Corporate to bank communication is still something that can count as a weakness in the system. With many corporates still following a set process for deal confirmation, it is easy to see how cracks can appear, making it easy for someone to access confidential and sensitive information.

Leavy says: "The online dealing systems are very good. Whether it is a bilateral or multibank system, the functionality is very important.

Executive summary

- Treasurers must identify the security controls they need to have in place and then use common sense to ensure that security-aware recruitment policies, segregation of process and the reduction of manual processes all lead to less fraud and more transparency.

- Working in isolation is not an option: treasurers need to bring in IT departments, HR and senior management to create and maintain an effective, secure organisation.

BOX 1. Fraud Act 2006

The Fraud Act 2006 came into effect on 15 January 2007, creating a new general offence of fraud that can be committed by false representation, by failing to disclose information, and by abuse of position. The Act also created the offences of:
- Obtaining services dishonestly;
- Possessing, making and supplying articles for use in frauds; and
- Fraudulent trading applicable to non-corporate traders.

Fraud (Trials without a Jury) Bill
The Fraud (Trials without a Jury) Bill was introduced into the House of Commons on 16 November 2006 to amend section 43 of the Criminal Justice Act 2003.
Source: the Fraud Advisory Panel. www.fraudadvisorypanel.org.

These tend to be very secure with deal capture and automatic confirmation."

A secure system is preferable to manual processes that will always be less secure. Leavy says: "Manual processes make it easier for significant loss to arise. If you don't have built-in interfaces and you are keying in information on a regular basis, then you are more at risk. Manual processes make it easier for somebody to circumvent the process itself."

Corporate treasurers need to examine how well protected their departments' processes are. Making sure that everyone is aware of the potential risks should be number one on the list. Each employee should know what part they have to play in preventing fraud.

Price says: "I don't think treasurers can address this issue on their own. It needs to be dealt with via discussions with IT and the board. It needs to be dealt with holistically, rather than in bits and pieces as a knee-jerk reaction. Each layer of security must be strengthened."

Changing attitudes and striving to find a more secure treasury management system could be a lengthy and costly process. Funding is often tight but making steps in this area could save you much more.

Julia Berris is a Reporter on *The Treasurer*.
editor@treasurers.org