# Preventing fraud – new technology, new risks

With an increasing reliance on new technology in the business world, the potential for catastrophic fraud is greater than ever, says Manson Garrick of Hibis Consulting.

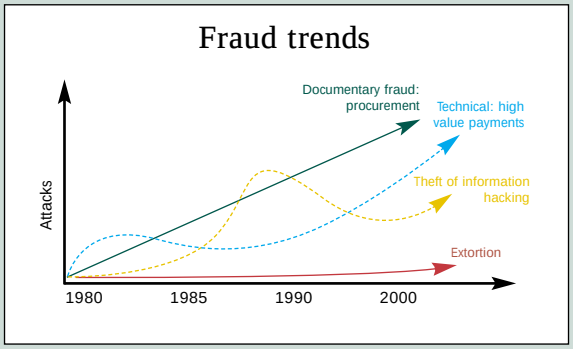
To many executives 'risk' is a four-letter word. Managers with the temerity to speak of fraud and risk in the same sentence, face the withering and acerbic wrath of management and colleagues alike. The reasons for this, while simple to understand, mask complex corporate and inter-personal relationships and ethics. Fraud is insidious and strikes at the heart of business and business relationships. It is complex, contradictory and an anathema to good management. The doctrine that good managers and rigorous controls prevent fraud is widely touted and the foundation for much corporate complacency.

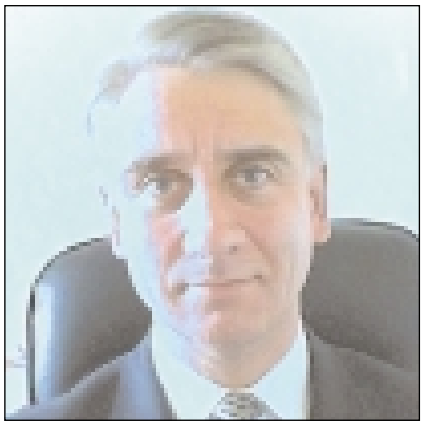
Fraud within retail markets is generally well controlled and managed across products as diverse as credit cards to mortgages and commercial lending to purchasing. It is seen as an inevitable component of doing business, a cost to be accepted, albeit grudgingly, provided tolerances and profit margins are maintained. It is an external attack on the company by clients, customers or third parties.

Corporate fraud attacks the heart of a business. It is employees, trusted staff, often working in collusion with external parties stealing from their employer. It is this betrayal of trust and breach of the core fabric of our working and personal relationships, which management finds so difficult to discuss or accept. Many management teams still believe that to plan corporate fraud prevention strategies is tantamount to admitting distrust of their colleagues and staff.

For these reasons, many businesses do not manage corporate fraud risks proactively, developing their anti-fraud arrangements only in response to specific incidents. This is particularly true of global businesses, which include treasury and other payment and settlement operations. When major losses occur, investigators and recovery specialists are parachuted in, often unclear of the business strategies and goals, resulting in unnecessary conflicts with line managers trying to limit credit exposure or maximise loss recovery, using their existing business framework. The results are internal confusion, lack of focus and mismanaged recovery.

*FIGURE 1*



Manson Garrick

### *Trends*

The threat of catastrophic fraud loss within areas of high risk such as treasury or other back office payment and settlement operations has increased significantly over the past 18 months, with an alarming rise in successful attacks. Contraction and amalgamations, high turnover in critical staff and advances in end-to-end processing have significantly changed the fraud risk profile of back office operations.

While the traditional view of fraud trends shown in *Figure 1* still holds true it will not be long before technical fraud overtakes documentary fraud as the primary target for crime gangs. The adoption by banks, finance companies and those associated with developing e-commerce businesses or business processes of data warehousing, electronic letters of credit and bills of lading as well as internet payment processes, contribute significantly to changing the fraud paradigm. A change already occurring in treasury where the automated through processing of transactions has shifted the fraud risk profile, moving the risks traditionally associated with the middle and back office to the front office.

Awareness of corporate fraud amongst senior and line management is still low. Few businesses have mapped critical fraud risks, depending on traditional controls and segregation of duties for protection. Countermeasures that are easily identified and bypassed by professional criminals.

### *Fraud programme*

The primary aim of a corporate fraud programme is the prevention and

detection of fraud and the recovery of undesired losses. A secondary aim is to help management achieve financial targets and corporate governance goals by assisting in reducing capital wastage, and by contributing to enhanced capital and shareholder value through improved (fraud resistant) systems, practices and procedures.

To achieve these goals, certain operating standards become critical and must be met by all staff. These include:

- **organisation:** roles, responsibilities and accountabilities for the prevention, detection and investigation of fraud and the recovery of losses must be clearly defined and communicated, both globally and at business levels;
- **policy:** policies and standards established for all fraud risks;
- **improvement:** the business must learn from mistakes;
- **knowledge:** transfer and dissemination of best practice;
- **risk management:** a complete and consistent process for measuring, controlling and reporting fraud risks as an integral part of the operating business;
- **solutions:** contact points for escalation of issues;
- **culture:** must promote fraud risk awareness by training, rewards and sanction; and
- **decisions:** risks identified for assessment and decision by appropriate levels of management.

These standards form the foundation for the development of cost effective prevention programmes. It is critical that managers first understand the level of risk they face and, more importantly, the appetite or tolerance which exists within the extended organisation for both the level of risk and the potential loss. This may include the views of directors and non-executive directors, institutional shareholders, regulators, rating agencies and major corporate clients, as well as internal risk managers and compliance and line management.

*Figure 2* suggests a high-level model, containing some of the key steps in the fraud risk assessment process.

A holistic view encompassing people, process and systems is critical, adding unique value by identifying loopholes seldom captured by traditional reviews of the control environment.

### *Fraud prevention*

Prevention seeks to establish a series of physical, logical and procedural barriers to discourage fraudulent attacks, implementing cost effective countermeasures to prevent or reduce the impact of the threat identified by risk assessment.

At the heart of any programme to prevent fraud is the effective, efficient and secure management of information in any form. Information is a key asset and is the product of people interacting with processing systems, technology and raw data. Protection may include one or more of the following elements:

- **confidentiality:** protecting sensitive information from disclosure;
- **integrity:** safeguarding the accuracy, completeness and source of the information;
- **availability:** ensuring information and services are available to users;
- **accountability:** ensuring users are properly authorised and can be shown to be accountable for their actions; and
- **auditability:** ensuring actions can be reconstructed and connected to a specific user or action, that compliance with key controls is verifiable and systems can be interrogated to confirm correct operation.

The weight attached to each of these elements will vary depending on the resource being protected and the threat.

Robust physical, environmental and corporate security controls are an integral part of information protection. They are also a primary measure in detecting and preventing theft and other losses and a key element in establishing acceptable standards of corporate care.

*FIGURE 2*

Key steps in fraud risk assessment

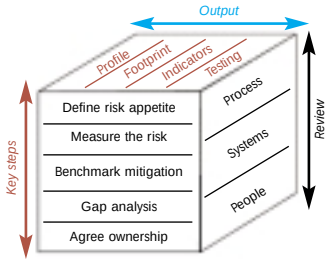
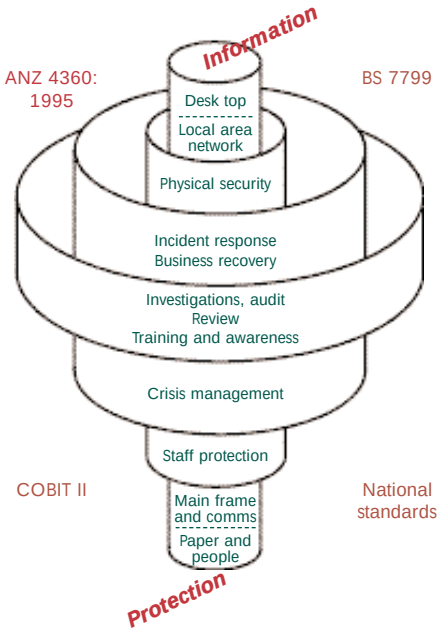



*FIGURE 3*

Fraud management programme




### *Fraud detection*

Detection aims at identifying losses or attempts to cause loss at the earliest possible opportunity and limit the amount of capital wastage. It includes:

- using a range of tools or techniques to pro-actively identify fraud such as:
  - filtering or data mining of accounting and procurement data;
  - fraud reviews (focused on specific risk areas);
  - risk mapping and assessment; and
  - intelligent or knowledge based systems;
- employee hot-lines and confidential reporting systems; and
- personnel security – including pre-employment screening and re-screening of existing employees, particularly those holding sensitive positions.

### *Investigation and recovery*

Recovery seeks to cost effectively and efficiently manage losses and other undesired incidents. A product of the recovery process is

also to learn from mistakes and identify weakness, in terms of people, processes or procedures and to develop effective countermeasures to prevent or reduce the likelihood of re-occurrence. Recovery includes:

- overt and covert investigations, interviews and management of external professional support;
- management of internal and external reporting relationships, including regulators;
- management of staff and internal corporate issues, including crisis management;
- preparation of corporate response to enquiries from media, shareholders or other external parties;
- presentation of findings to board and senior management and, where appropriate, external regulators or other agencies;
- identification of procedural weaknesses or differences in policies and practices, developing action plans to mitigate these issues; and
- transferring knowledge (and best practice learning points from the incident) through training and awareness programmes.

*Figure 3* shows the relationship and integration between the main elements of a fraud management programme, much of which will already be well-established in most business operations.

***Keep on your guard***

The level and sophistication of attack is increasing and as businesses move into e-commerce and greater dependence on technology the fraud paradigm shifts, increasing the risk of catastrophic loss.

Businesses should assess their critical risk areas, identifying and establishing tolerances for both the level of risk and potential loss.

Countermeasures should be realigned to achieve robust protection and best value for money. Continuous review, assessment and adjustment should become the norm rather than the exception for businesses wishing to maintain competitive advantage. ■

*Manson Garrick is a Director and co-founder of Hibis Consulting Limited. He was formerly Managing Director of Consulting, Network Security Management and Group Head of Security Risk Management at Standard Chartered Bank.*