Fraud Advisory Panel
12th Annual Review 2010

Managing the risk of fraud

The Fraud Advisory Panel acts as an independent voice for, and supporter of, the counter-fraud community. It exists to raise awareness of the immense human, social and economic damage caused by fraud and to help individuals and organisations to develop effective fraud prevention strategies.

Contents

The Fraud Advisory Panel encourages a truly multi-disciplinary perspective on fraud, with members drawn from the public, private and third sectors, and from across a variety of professions.

No other organisation has such a range and depth of knowledge, both of the problems and of the solutions. By bringing together people and organisations with an interest and expertise in preventing, detecting, investigating and prosecuting fraud, we believe that we can make a real contribution to stopping fraudsters in their tracks.

The Panel was established in 1998 through a public-spirited initiative by the Institute of Chartered Accountants in England and Wales (ICAEW). Today it is a registered charity and company limited by guarantee, funded by subscription, donation and sponsorship.

The Panel's work includes:

- Advising business and the public on prevention, detection and reporting.
- Originating and responding to proposals to reform the law and public policy, with particular emphasis on investigation and prosecution.
- Improving education and training in business and the professions as well as amongst the general public.
- Establishing a more accurate picture of the extent, causes and nature of fraud.

Chairman's overview

A strategic approach to fraud risk management

Everyone has a role to play in managing the risk of fraud in both their personal and professional lives. And this is the theme of this year's Annual Review, focusing principally on the steps that can be taken to reduce the chances of becoming a victim.

For businesses, nothing less than a truly concentrated approach will do. Good fraud risk management is now an essential part of good corporate governance, and fraud should be high on every organisation's agenda, whether in the public, private or third sector. Fraud risk should be included in every risk register and reviewed regularly at board meetings.

But that isn't the end of it: private individuals are no less at the mercy of fraudsters, more often than not unwittingly. What steps should they be taking to protect themselves? The first step is to let people know what risks they face. The Home Secretary has recently identified some key areas of fraud which can hit each one of us and highlighted the dangers which law enforcement is increasingly under pressure to tackle: bogus share-dealing, sale of fake events tickets, fraudulent property rentals and fake dating sites. Other, more traditional risks, still remain: identity fraud, fake lotteries, advance fees for non-existent loans and prime bank guarantees.

People obtain information from a variety of sources; predominantly television and the popular press. Apart from the excellent *The Real Hustle*, there is very little publicity given to common scams on TV. There is a need for a concerted media campaign to highlight traps for the unwary. This would go a long way to prevent more of us falling victim to the sharks and swindlers out there.

The need for effective law enforcement to tackle the fraudsters who have slipped through the prevention net has been underlined by the Panel over the years. It is needed now more than ever when the police, like other public bodies and government departments, are being told they must take a 20% cut. Financial crime has never been high up on the government's agenda and it is reassuring to hear the Home Secretary vowing to crack down on *"middle-level"* fraud. But incorporating fraud officers in an 'FBI-style' National Crime Agency (NCA) risks them being diverted to other tasks seen as more serious or pressing. This has happened time and time again when chief police officers disbanded their dedicated fraud squads or rolled their resources into 'major crime units' to address local policing priorities.

The government has declared its determination to sweep away *"the confused multi-agency approach"* to fighting fraud, and is now looking at the potential shape and remit of a new unified economic crime agency. Our own discussion document – *Roskill Revisited: Is There a Case for a Unified Fraud Prosecution Office*? – has recently examined this very need. The success of any such agency will, as always, hinge on how well it is resourced and what tools it has at its disposal. Talk of separating the SFO's investigation and prosecution roles has raised deep concerns among those who remember the near impossibility of bringing home a serious fraud prosecution in the days before Roskill.

Questions of alternative sanctions, negotiated settlements, and even the retention of penalties by partially self-funding prosecutors, have divided fraud fighters. Alternative remedies do deliver lower investigation costs and this is to be welcomed. But a series of penalties seen by many as over-lenient has left the impression of a two-tier justice system which lets corrupt executives off lightly but sends benefit cheats to jail.

More proportionate and more certain penalties, an objective awareness of prosecutorial conflicts of interest, and a keen eye for questions of value over price are all needed if the criminal justice system is to have its capacity to deter fraud restored. It is unlikely that this can be done properly *and* on the cheap.

Rosalind Wright CB QC
June 2011

Key achievements 2010

Advising and informing

The provision of advice and information is the cornerstone of the Panel's work.

- A comprehensive redesign of our website (www.fraudadvisorypanel.org) greatly improved accessibility to its wealth of practical advice and up-to-date information, all of which can be downloaded free.
- The ten new titles added to our popular *Fraud Facts* series include guides to spotting and avoiding online shopping scams, boiler-room investment frauds and ponzi schemes, as well as introductions to good practice in fraud risk management, parallel sanctions, fraud response plans and anti-fraud policies.
- Specialised publications also looked at the practical and legal challenges of recovering assets from overseas jurisdictions, and recovering and realising art assets.
- The Panel contributed articles to a number of external publications and provided expert media comment throughout the year.

Influencing

The Panel plays a very active role in stimulating and informing wider discussion and debate about fraud prevention, detection, investigation and prosecution. In 2010 this included two special projects and contributions to a number of government consultations.

- *Fraud Reporting: A Shared Responsibility* examined UK listed companies' existing obligations to prevent, detect and report corporate fraud. A comprehensive review of legislation, regulations and guidance was followed by a pair of stakeholder forums involving more than 50 business leaders and senior figures in law enforcement, regulation and professional services (see page 20).
- *Roskill Revisited: Is There a Case for a Unified Fraud Prosecution Office?* asked if the original recommendations of Lord Roskill's 1986 Fraud Trials Committee – to create a unified fraud prosecution office and independent oversight body – might improve fraud prosecution today and facilitate a more coherent national anti-fraud strategy.
- Responses were submitted to three government consultations: *Policing in the 21st Century; E-Consumer Protection; A New Approach to Financial Regulation.*
- Advice, information and support was given to the National Fraud Authority, particularly in relation to its efforts to assess the impact of fraud on small and medium-sized businesses (SMEs).

Training and educating

The Panel believes passionately in the importance of counter-fraud education and training for all, including within business and the professions.

- 16 events delivered an extensive training programme for counter-fraud professionals in all sectors. Topics included plea negotiations, bribery and corruption, the Fraud Act 2006, fraud response planning, and asset tracing.
- A participative workshop in practical fraud detection visited London, Birmingham and Leeds.
- Collaboration with the Chartered Institute of Internal Auditors – UK and Ireland (CIIA) continued with our joint annual conference *(Combating Fraud in the Current Economic Climate)* and a pair of one-day training courses on *Fraud Risk and the Internal Auditor.*
- An executive breakfast briefing in collaboration with the Association of Certified Fraud Examiners (ACFE) looked at *Conducting Successful Fraud Investigations.*
- Expert speakers were provided to 21 external conferences, including events convened by the ICAEW, CIIA, Community Accounting Network, and British Bankers' Association.
- The Panel's regional presence was greatly expanded by the launch of regular practitioner meetings in Birmingham, Bristol, Edinburgh and Leeds. Members and guests gather to hear visiting speakers and to share information, experiences and best practice.

About the Panel

Governance

The Panel is governed by a board of trustees which meets six times a year. It is supported by two full-time members of staff. Its manager, Mia Campbell, is responsible for the day-to-day management of the organisation.

Much of the Panel's detailed work is carried out by volunteers who give their time and expertise via a range of multi-disciplinary groups which meet regularly:

- Asset Recovery: considers issues relating to the use of criminal and civil redress in order to recover assets.
- Cybercrime: improves awareness and understanding of e-crime and how to safeguard against it.
- Fraud Investigation and the Legal Process: examines issues relating to the investigation process, criminal and civil procedures, arbitration and mediation.
- Fraud Prevention and Detection: promotes best practice in fraud prevention and detection and works to improve fraud awareness amongst business, the professions and the general public.

Regional members groups also meet regularly to discuss local issues and to contribute to Panel projects.

Benefits of membership

- Influencing public policy through the Panel's proposals and recommendations to government.
- Networking and opportunities to exchange information and share best practice with like-minded professionals and to hear from guest speakers.
- Participating in multi-disciplinary groups on topical fraud issues.
- Preferential rates for conferences, seminars and workshops.
- Working in the public interest to address the concerns of business, the professions and the general public.
- Regular updates on Panel activities and the latest developments in the counter-fraud arena.

Corporate membership includes up to 20 named employees entitled to all of the above benefits as well as:

- Preferential rates for Panel events, applicable to all employees.
- Public acknowledgement on the Panel's website.
- Use of a special 'corporate member' logo on company stationery and websites.
- A free professional training session on a fraud-related subject of choice.

Getting involved

People and organisations join the Fraud Advisory Panel because they are concerned about the problem of fraud and want to do something about it. The Panel has over 40 corporate members and 280 individual members. All members are required to comply with a code of conduct.

We invite you to become part of our highly-respected organisation today. For more information about membership please contact the Fraud Advisory Panel on 020 7920 8637 or membership@fraudadvisorypanel.org.

Supporting the Panel

The Panel gratefully acknowledges the support of all members who have given generously of their time and expertise.

In addition we would like to extend special thanks to AlixPartners, Baker Tilly, Challinors, Clydesdale Bank, Deloitte, Ernst & Young Grant Thornton UK, KPMG Belfast, Moore Stephens, National Audit Office, PKF (UK), Smith and Williamson, and RSM Tenon, all of whom provided venues and/or sponsorship.

For more information about sponsorship opportunities or event hosting please contact the Fraud Advisory Panel on 020 7920 8637 or events@fraudadvisorypanel.org.

Trustees

Ros Wright CB QC
Chairman
Member and past chairman of the supervisory committee at OLAF (the European Anti-fraud Office); independent member, Department for Business Innovation and Skills insolvency service steering board; complaints commissioner of the London Metal Exchange; vice-chairman, Jewish Association for Business Ethics; bencher of the Middle Temple; director, Serious Fraud Office 1997-2003.

Phillip Hagon QPM
Head of corporate security at Sainsbury's with responsibility for security strategy. Thirty-three years with the Metropolitan Police Service, retiring with rank of commander. Awarded the Queen's Police Medal for Distinguished Service in 2005. Liveryman of the City of London.

Felicity Banks
Head of business law at ICAEW specialising in economic crime; represents the accounting profession on HM Treasury's money laundering advisory committee; chairman, accountants affinity group of the Anti-Money Laundering Supervisors' Forum.

Barbara Hart
Chartered accountant; former charities manager, ICAEW 2007-2008; former finance director of CARE International UK 1998-2001 and the Mothers' Union 2001-2007.

Alex Plavsic
Head of forensic services at KPMG. During 20 years at KPMG Alex has worked on many high profile cases including Polly Peck, Grupo Torras and the investigation of Jeffrey Archer in relation to the Simple Truth appeal. In the last four years several of Alex's cases have involved bribery and corruption matters including presenting to the SEC and SFO.

David Clarke
Detective chief superintendent and director of City First, the City of London Police's transformational change programme; former director of intelligence, head of the National Fraud Intelligence Bureau, and member of the original Fraud Review team.

Dr Stephen Hill
Chairman, Cybercrime Working Group
Managing director of Snowdrop Consulting Ltd; independent consultant and lecturer specialising in fraud and e-crime; honorary steering committee member, London Fraud Forum; volunteer, Police Support Volunteer Programme; associate, Association of Certified Fraud Examiners; affiliate, Institute of IT Trainers; CIIP certified.

Monty Raphael QC
Chairman, Fraud Investigation and the Legal Process Working Group
Special counsel at Peters and Peters, specialising in domestic and international business crime and regulation and acknowledged as the *"doyen"* of the UK's fraud lawyers; honorary solicitor, Howard League for Penal Reform; visiting professor of law, Kingston University; editor, Blackstone's Guide to the Bribery Act; lecturer on fraud-related issues.

Corporate members

- Alico Management Services Ltd
- AlixPartners UK LLP
- AON Ltd
- Association of Certified Fraud Examiners
- Association of Certified Fraud Examiners (UK Chapter)
- Association of Chartered Certified Accountants
- Aviva plc
- AXA Sun Life
- Baker Tilly
- BDO LLP
- Beever and Struthers
- Cadbury
- Chantrey Vellacott DFK LLP
- CIFAS – the UK's Fraud Prevention Service
- Control Risks Group
- Credit Agricole Corporate & Investment Bank, London Branch
- Deloitte LLP
- Ernst & Young LLP
- Experian Decision Analytics
- Financial Services Authority
- Haslocks Forensic Accountants Ltd

Bill Cleghorn
Deputy chairman
Director of Kinetic Partners LLP (asset management) and director of Aver Corporate Advisory Services Ltd (non-asset management), specialising across all sectors in fraud and financial crime investigation and corporate recovery; director, London Fraud Forum; fellow, Association of Business Recovery Professionals; lecturer on fraud-related issues and money laundering.

Will Kenyon
Partner in the forensic services group, PricewaterhouseCoopers LLP; founding head of forensic investigations, PricewaterhouseCoopers Germany 1998-2001; specialising in the prevention, detection and investigation of fraud and financial crime across most industries, both private and public sector; involved in investigations and recovery actions in relation to some of the most significant fraud and corruption cases of the last 20 years.

Neil Griffiths
Partner in the reconstruction and insolvency group at SNR Denton, specialising in contentious and fraud-related cases; former vice chairman, creditors' rights committee, International Bar Association.

Steven Philippsohn
Chairman, Asset Recovery Working Group
Former deputy chairman of the Fraud Advisory Panel; founder and senior partner of city solicitors, PCB Litigation LLP, specialising in national and international fraud litigation and asset recovery; UK representative member of Fraudnet, the fraud network of the International Chamber of Commerce.

David Skade
Director within the global anti-money laundering risk management team for Bank of America Merrill Lynch covering the Global Wealth and Investment Management teams across the EMEA region; former MLRO at Credit Agricole CIB and HVB AG; wide background across many aspects of banking involving internal audit investigations, operational risk control, fraud investigations and front office lending activities.

Staff

Mia Campbell
Manager

Oliver Stopnitzky
Executive

Consultants

Martin Robinson
Education and training consultant
Chairman, Fraud Prevention and Detection Working Group

David Ovenden
Website and database consultant

Special thanks to Jonathan Fisher QC who served as a trustee director until 6 July 2010.

- ICAEW
- Institute of Chartered Accountants of Scotland
- International Compliance Training
- Kennedys
- KPMG LLP
- Law Society of Scotland
- Lawrence Graham LLP
- Lloyds Banking Group
- McGrigors LLP
- National Audit Office
- National Fraud Authority
- Northern Ireland Audit Office
- PKF (UK) LLP
- PricewaterhouseCoopers LLP
- Prudential plc
- Royal and Sun Alliance plc
- RSM Tenon
- SNR Denton
- The Cotswold Group Ltd
- Transport for London
- UBS AG
- Wolters Kluwer Financial Services

The true costs of fraud

We are all victims of fraud on the epidemic scale now witnessed. Fraud weakens the very fabric of civilised society by undermining trust. It attacks prosperity through higher prices, stiffer taxes and reduced public investment.

The National Fraud Authority's (NFA) figure for total UK fraud losses (£38.4 billion) is a staggering £765 for every UK adult. Organisations – public, private and third sector – shoulder much of the burden, but individuals still lose an estimated £4 billion a year to fraud.

Some fraud remains hidden – undetected and unreported – but the largest items missing from the reckoning are the cost of preventing and responding directly to fraud and the psychological and emotional costs of victimhood, which can be profound and disabling.

So the cost of fraud extends far beyond the purely financial. In the worst cases something beyond price is stolen along with the money. Victims (and others touched by the crime) report deep and debilitating feelings of anger, resentment, embarrassment, disgust, powerlessness and humiliation; feelings that can persist long after the financial pain has eased.

The Fraud Advisory Panel was one of the first organisations to draw attention to the plight of victims of fraud as part of its 7th annual review and 2006 paper on *Victims of Fraud*. There is now compelling evidence that victims have not been getting the support they need and deserve. This is changing, and the Panel applauds that. But if we care about the wider impact fraud has on society, and if we want to build the most accurate picture possible of fraud, then we can still do more to support victims and reduce their distress.

Consumers beware!

Boiler-room fraud
Crooks select their targets from UK shareholder lists, then cold-call their victims, inviting them to buy shares or currency options which are in reality worthless. Thousands have been caught in this way. The biggest individual loss recorded so far by the National Fraud Intelligence Bureau (NFIB) is £1.2 million. The fraudsters target their UK victims from overseas, using armies of jobless youngsters often based in large open-plan offices (the 'boiler-rooms') and reading from prepared scripts. New strategies are now re-targetting old victims, promising to recover the money they've already lost to the original scam or offering to buy back the worthless shares – but always for an up-front fee.

Advance fee fraud
This technique works by enticing victims to pay in advance for a non-existent benefit. The tempting reward might be a lottery win, a dream job or even the perfect date. But first the victim must make an up-front payment; an administration fee, 'federal taxes' or a service charge. Once the money has been paid the fraudsters disappear into thin air, taking the 'prize' with them.

High-yield investment fraud
With conventional interest rates as low as they have ever been, the siren voices of crooks offering attractive returns on unusual investments are simply too alluring for some to resist. 'Prime bank guarantees' (normally available only to banks who trade them with each other – or so the pitch goes); fine wines, champagnes or whiskies (for resale at a large profit later); pockets of undeveloped land (big gains when planning permission for housing is secured); all these are typical vehicles for the high-yield scam. But the so-called investments are merely figments of the fraudster's fertile imagination, and the unwary are duped every time.

Is fraud simply a cost of doing business?

Fraud, with its legacy of shame, distrust and fear, strikes at our sense of self every bit as much as it strikes at our bank balances. And this is as true for organisations as it is for individuals. Fearful of what markets, customers, competitors and suppliers might think, many businesses guard carefully the privacy of their own victimhood.

In the fight against fraud this is as unhelpful as it is insidious. It encourages the belief that fraud *"doesn't happen around here"*; that in any case it can be tackled as-and-when, on an *ad hoc* basis; that it is somehow a discrete and isolated threat, with limited or no consequences for the health of the total organisation. But the devastating consequences of fraud stretch far beyond an organisation's economic loss to include the impact on staff, shareholders, customers and wider society.

Paying the price

The 'corporate cost' (put at £12 billion a year by the NFA) is ultimately shouldered by us all, as customers and shareholders. In straitened times, prices made artificially high by fraud result in tangible welfare losses, especially for those who can least afford them. And when the true picture of poor fraud prevention and data security finally leaks into the public domain, the reputational damage it causes must be carried by shareholders and employees as their returns and job prospects decline.

Fear of fraud stunts overall economic activity and growth too. Half of Britons are seriously concerned about the security of shopping or banking online (Unisys Security Index, February 2011), and the fear of fraud and corruption is thought to discourage half of companies from moving into new foreign markets (Kroll Global Fraud Report, 2010/11).

Meanwhile, the Financial Services Authority (FSA) notes that companies struggle to calibrate their anti-fraud investments properly because the full implications of fraud risks, including the hidden costs, are not taken into account by standard return-on-investment (RoI) calculations.

Failing health

In the public sector the link between fraud losses and reduced benefits is even starker.

One piece of research recently estimated that the NHS is losing at least £3.3 billion to fraud each year. That's 3% of its total budget; the same amount it spends on cancer drugs, hip replacements, cataracts and dentistry combined. The NFA estimates that fraud costs UK taxpayers £15 billion each year in lost tax revenues. Various other forms of fraud and evasion siphon off another £2.6 billion from central government and £2.1 billion from local councils.

Is fraud *really* an acceptable cost of doing business? Or is there a need for a new way to talk about and account for the true burden of fraud losses?

New frontiers
21st century fraud risk management

At the corporate level, anything less than an organisation-wide approach to fraud risk management is increasingly out of step with the demands of modern business. Ours is a world resonating with new and unfamiliar fraud risks that challenge organisations throughout their operations and activities.

The Web 2.0 revolution of smartphones, wireless networking and social media empowers the fraudster, terrorist and organised criminal to a fearsome extent.

The Bribery Act 2010 for the first time holds UK businesses responsible for acts performed in their name anywhere in the world. Does it also point to a future in which ethical regulation increasingly sets the parameters of acceptable business behaviour at home and abroad?

Non-financial factors have come to define public perceptions of an organisation and, through them, the value placed on it by the markets, redefining the risk landscape in the process.

Unusual forms of value – carbon credits, renewable power, fair trade, sustainable technologies – are difficult to price and make secure. Old business certainties can no longer be taken for granted.

The globalised market

The growing realisation that this is 'one world' – and a small one at that – changes everything. Criminal gangs, like many of their corporate victims, operate with apparent ease across borders. Their malign and corrupting influence helps to create failing states, ensure persistent poverty and fund terrorism all over the world.

New domestic legislation, like the Bribery Act 2010, is in fact designed for globalised business, explicitly recognising the ethical risks embedded in unfamiliar foreign markets and practices, and then reaching out to police them.

A watershed Act

Indeed, the new Bribery Act 2010 promises to be a watershed in ethical regulation. Successful international financial and business centres need not just technical skill but probity too. Businesses must now expect to be held to higher ethical standards wherever they operate. The Bribery Act's extensive guidance also provides organisations with a detailed self-help guide to building, maintaining and applying an ethical business culture which will help to prevent fraud as well as corruption.

The Bribery Act: a model for fraud risk management?

The Ministry of Justice guidance that accompanies the Bribery Act 2010 reads like a best practice guide to fraud risk management in general, not just bribery and corruption. Under its six principles, the guidance encourages procedures that are proportionate, appropriate and pro-active.

Principle 1. Proportionate
Anti-bribery procedures should be proportionate to the risks faced and the nature, scale and complexity of the organisation's activities.

Principle 2. Top-level commitment
Senior management is committed to and active in preventing bribery, working to foster a culture in which the practice is never acceptable.

Principle 3. Risk assessment
The organisation makes regular, well-informed and clearly documented assessments of the risks it faces.

Principle 4. Due diligence
The organisation applies due diligence procedures in selecting agents and contractors, both as a form of risk assessment and a means of mitigating that risk.

Principle 5. Communication (and training)
Through internal and external communication and training, the organisation seeks to ensure that bribery prevention is embedded and understood throughout the organisation.

Principle 6. Monitoring and review
Anti-bribery procedures are monitored and reviewed so that they can be improved where necessary.

The corporate response to the Bribery Act 2010 has already included a much wider deployment of compliance functions outside the financial services sector. These are now adding value in other areas of risk management including, for example, anti-fraud and anti-competitive behaviour. This very positive development is a direct result of the Act.

Green fraud

The 'greening' of business practice is unfamiliar territory for most organisations, making businesses vulnerable to 'green' scams as they try to fulfil their growing environmental and social responsibility obligations (see box).

Many organisations believe that non-financial reporting is not a proper concern for fraud risk management. We disagree, and so it seems does the Bribery Act 2010. Its detailed guidance implicitly recognises that where a company's environmental and social activities are closely linked to its commercial life (and they almost always are) the risk that one will corrupt the other is very real. It also notes that an unfairly acquired commercial advantage can take many forms: not just a contract won, but an environmental regulation waived, a community responsibility forgotten, a safety inspection indefinitely postponed.

Investors increasingly see the long-term prospects of a business reflected as much in practical demonstrations of its ethical life – environmental stewardship, social responsibility, health and safety – as in its balance sheet or profit and loss statement. Enlightened executives are right to be concerned about the accuracy and trustworthiness of the non-financial information they release to the world. To satisfy the needs of management, stakeholders and regulators, it does need to be reliable, honest and accurate – and conspicuously so. But the novelty and immaturity of non-financial reporting makes it an ideal place in which fraud and deception can take hold. For example:

- 'cherry picking' to report only successes;
- changing the measurement basis to distort year-on-year analyses;
- changing key spreadsheet assumptions to improve outcomes;
- choosing less rigorous or inexperienced audit providers.

It is true that difficulties with measurement, presentation, standards and conventions dog this new area of corporate reporting. But these are the vulnerabilities that trouble all new areas of thought and practice. They are not reasons to take non-financial fraud risk management less seriously. Rather, the opposite is true.

Fraud plagues climate change response

As soon as the 1997 Kyoto Protocol put a price on carbon emissions the first carbon trading fraud became an inevitability. The problem became so serious that in January 2011 trading on the EU's exchange (which conducts 80% or so of global trading volume) was suspended until minimum security standards were in place across all member states.

Fraudsters had been hacking into poorly secured national carbon registers and stealing credits for resale on the open market. In the first three months of 2011 credits worth some 50 million euros were stolen from registries in Eastern Europe. The thefts were so big and complicated that organised crime rings are suspected. Perhaps the most audacious attack was in the Czech Republic where criminals used a bomb scare to clear the registry building of staff.

Simple email phishing techniques (such as asking organisations to re-register) have also been used to access accounts illegally and steal carbon credits. Carousel frauds have used carbon credits to exploit differences between national tax rules and steal VAT remittances. The lack of a common EU-wide registry of allowances and credits has made it possible to double-sell carbon credits to unsophisticated buyers.

Companies can meet some of their carbon compliance obligations using credits earned supporting sustainable development projects (CDM) in poorer countries. This scheme is vulnerable to the same risks as carbon trading, but also carries a high bribery and corruption risk because of the link to the economic viability of the underlying project.

A special type of project-based carbon credit (REDD – Reducing Emissions from Deforestation and Forest Degradation) was designed to create a financial incentive to protect the world's forests. Qualifying projects are often in remote locations in countries which lack transparency, increasing the risk of fraud and corruption. At present REDD projects are limited to the voluntary carbon trading market in which a lack of regulation adds to the risk of fraud.

Cybercrime

Cybercrime is now the second largest threat to the UK after terrorism. It costs a staggering £27 billion each year. Intellectual property theft and industrial espionage are the biggest areas of loss; business is the biggest victim.

Just a handful of years ago the term 'cybercrime' had yet to be coined. Two things changed. Networking came of age, and the new generation of Web 2.0 applications made child's play of information sharing and online collaboration. Wireless devices provide powerful new ways to access and manipulate web-based information and services, on the move, anywhere in the world.

Advances like these reshape the business world so fast there is hardly time to consider the downside. But while most of us barely scratch the surface of the functionality in our pocket, the fraudsters systematically mine technological innovations for every possible advantage.

- Over-the-counter face recognition software and hacking can match real people to their personal information held online so that they can be defrauded, blackmailed or recruited into committing a crime (probably against their employer).
- Fake wireless hot-spots and WiFi portals, set up invisibly in public places, harvest personal data and private communications from passers-by and local businesses.
- Industrial espionage – the theft of sensitive competitive information about contracts, tenders, mergers and acquisitions – costs UK business more than £7.5 billion every year. Financial services, aerospace/defence and mining are the biggest victims.

- Intellectual property worth £9 billion is lost to fraudsters every year, much of it from the health/pharmaceuticals/bio-tech, IT and electronics sectors.
- Denial of service attacks – using malware to flood a corporate server with bogus messages – are used to hold businesses to ransom, threatening to cripple their IT infrastructure and bring their operations to a halt. Annual losses: £2.2 billion.

Stuxnet worm

The Stuxnet 'worm' (a complex computer code), which specifically targeted industrial control systems, revealed that hackers now possess unprecedented power to manipulate real-world industrial and security equipment without the operators' knowledge. Worryingly, the attack targeted Siemens systems widely used around the world to control nuclear and gas infrastructure, as well as in manufacturing and the automotive industry.

Data security

The Cabinet Office puts the cost to businesses of customer data loss at between £1 billion and £1.4 billion. Government departments and businesses have until recently had very little incentive to take data security seriously, and it shows. A recent survey of London's 71 health trusts by a UK national newspaper found 909 data security breaches in the last three years among the 30 trusts that supplied data. Most had been caused by avoidable staff error.

In an age when an organisation's business plan, its R&D blueprints, the personal details of every staff member and the bank details of every customer will all fit on a device the size of a child's thumb, we all need to ask *"how secure is our data?"*

Changes to the Data Protection Act have now created new and compelling incentives to take the risk of data loss seriously. The maximum penalty for failing to protect data has been raised 100-fold to £500,000. The growing trade in personal data has led the government to consider criminal sanctions, with a maximum penalty of two years in prison for the most serious offences.

British businesses, consumers and governments have been happy to reap the *rewards* of the latest generation of computer and communications technologies. Now it is time for a 21st century approach to managing the cyber *risks* that accompany them.

Vulnerable data

The security risks associated with the concentration of massive amounts of personal information were starkly illustrated by recent events at Sony. Hackers stole the personal details of 77 million online PlayStation Network gamers and 25 million Sony Online Entertainment customers. The missing data included debit card records, names, email addresses and telephone numbers – all rich pickings for fraudsters.

Head in the clouds

Cloud computing – in which corporate data and applications reside on third-party servers and are then accessed on-demand by users – promises a host of business benefits, especially lower costs.

But clouds bring together vast quantities of valuable data, from thousands of users, into a structure that is designed to be accessible from anywhere, by anyone. In other words, not only are they prime targets for fraudsters and data thieves, their relatively weak access and authentication systems make them soft targets too.

Cloud clients must of necessity place enormous amounts of trust in third-party systems and staff. Be sure you've done your due diligence. Select a cloud with demonstrably strong security and efficient systems for addressing breaches. And make sure your own staff ID and data access management systems are sharp and reliable too.

Social media

Whether an organisation exploits social media for business purposes (market monitoring, boosting web traffic, raising awareness), is simply concerned to prevent inappropriate use by staff, or both, the key risks are the same: data leakage, information theft, espionage, reduced productivity, and the threat from malicious software (malware). Controls like strict prohibitions and access restrictions can be ticklish to enforce sensitively. But frequently all it takes to get staff on-side is better awareness training on the risks that all of us, individuals and organisations alike, routinely encounter in cyberspace.

Seven practical steps to help secure your business against cybercrime

- Start writing your IT security plan now. Aim for something that delivers benefits quickly – you can perfect it later. And don't neglect physical security for systems and data.
- Control internal access to critical information and review access privileges regularly.
- Staff use of memory sticks, WiFi and smart phones all present exceptional security risks in the workplace. Consider an outright ban, or at the very least implement strict controls.
- Use secure encryption to protect information travelling over the public internet; strictly control and review remote access to the corporate network.
- Train all staff in the principles and best practice of IT and data security; make it part of induction; underscore personal responsibilities.
- Write good staff policies to cover use of the internet (including private use), email systems (including webmail), passwords, laptops and portable devices, personal software, sharing and downloading of copyright material, and details of monitoring procedures; explain what happens when these rules are breached.
- Cut 'cyberslacking': monitor internet use, install internet content filters, restrict access to browsers and email, and strictly control software installations.

Corporate identity fraud

Identity fraud is constantly in the news. The threat was once limited to individuals, but now it is a growing problem for companies too.

Companies House estimates that between 50 and 100 cases of corporate identity fraud occur each month.

By pretending to be an authorised person fraudsters take control of the company's bank accounts, credit cards and confidential information, using them to siphon off cash and assets. They may set up bogus merchant accounts and steal the supplies, register similar website domain names to hijack on-line revenues, or simply file false paper returns at Companies House to create the impression that they are directors of the business. A host of simple but effective ruses like these could be costing SMEs some £1.3 billion a year, according to one insurance industry survey.

The best defence is vigilance.

- Check your website and Companies House records regularly. Sign up for Webfiling, PROOF and Monitor services.
- Reconcile bank and company credit card statements meticulously.
- Review your company's credit report regularly.
- Set strict staff guidelines about who can order things on behalf of the company and what information they can give out.
- Make it easy for staff, customers and suppliers to report anything unusual; encourage a 'no blame' staff culture so that issues are discussed openly and without recrimination, not buried.
- Monitor domain name registrations similar to yours. Consider registering common misspellings and variations yourself.
- Use a variety of sources when checking the *bona fides* of new customers or suppliers.

People risk

Whilst the majority of staff are honest and hard-working, the few that are not continue to present a major fraud threat to their employers.

Half of all frauds against businesses are believed to be perpetrated from within (PwC, 2009). The database compiled by CIFAS – the UK's Fraud Prevention Service shows that in 2010 staff fraud was more than 40% above its 2008 level. Instances of staff illegally obtaining or disclosing personal data had increased 63% compared with 2009. No wonder the Association of Certified Fraud Examiners (ACFE) reports that a typical organisation loses about 5% of its annual turnover to staff fraud.

The importance of employment screening as part of a business's fraud risk management toolbox has arguably never been greater *(see: The dos and don'ts of pre-employment screening)*. Within the financial services sector it is estimated that 15% of CVs contain some kind of discrepancy. But the management of people risk is more than just trying to avoid recruiting bad people and ejecting those that turn bad later on.

A two-way street

The workplace fraud risks that some people create through their behaviour and their influence on business practice is just one side of the people risk coin. The other is the impact that an organisation's culture, processes and systems may have on the ethical behaviour of those who work there.

A person doesn't have to be morally corrupt to find themselves in deep ethical water. They may simply have been badly informed, badly trained, badly managed or badly led.

Raison d'être risk

Each of us needs to know what it is that we are supposed to be doing and what 'right' really looks like. This isn't always obvious. In the fluid, last-minute culture of modern business it's all too easy to misunderstand what's really expected of us – especially where policies and practices are poorly defined or poorly communicated. The more complex or stressful the situation, the harder it is to be sure of what really matters and what is 'right'.

Competence risk

Often people are chosen for reasons other than competence (who they know, perhaps, or how much they are worth). Through no fault of their own they can find themselves without the skills to discharge their new responsibilities efficiently and securely. Then they become risk hotspots, vulnerable to corner-cutting, poor judgement and mistakes. Managers promoted beyond their practical or ethical abilities magnify these same risks through the teams they direct and influence.

Domestic risk

The distinction between home and work is not what it was. But just as many employees habitually take their work home with them, so they bring their domestic concerns into the workplace. Support at work for staff with debt or other money worries at home can help reduce the risk that they will try to solve their problems alone and by criminal means.

Reward risk

Rewards, incentives, and disincentives too, all need to be aligned with the long-term interests of the organisation. Social psychologists have repeatedly shown that ethical behaviour is closely informed by the social setting. A workplace optimised to minimise people risk blends the hard controls of traditional risk management with softer, enabling structures (training, development, incentives, rewards) that support employees' instinctive desire to do the right thing.

The dos and don'ts of pre-employment screening

- Screen everyone: permanent and temporary, high and low.
- Make all your checks *before* the employee starts work.
- Checks should be proportionate to risks.
- Assign formal staff or departmental responsibility for the process.
- Ask all prospective employees to sign a full consent form and data protection statement.
- Verify these as a minimum:
  – identity
  – address
  – qualifications
  – employment history
  – right to work in UK
- And preferably these:
  – criminal history
  – financial background
- Keep the process simple and inexpensive by using online sources or direct approaches.
- Always take up references, and follow up any that don't materialise. Don't let yourself be charmed into not checking.
- And new employees are not the whole story: consider checks on existing employees when they are promoted into positions of greater responsibility or exposure.

The FAP has published a Fraud Facts guide to pre-employment screening. It can be downloaded from the FAP website at:
www.fraudadvisorypanel.org/new/publications

Taking a holistic approach

The time has come for organisations to take a properly 'holistic' approach to fraud risk management. Simply stated, good fraud risk management practice should run through an organisation like the lettering in a stick of seaside rock. It should be a set of ideas, principles and practices which are so deeply embedded that they underpin everything an ethical, secure and risk-aware organisation does, and is.

Technology has digitised who we are and made it available to every crook with an internet connection. Globalisation opens the door to new worlds of business with unfamiliar rules, or no rules at all. Budget cuts and uncertainty about the future of almost every regulator or law enforcement agency have weakened our already-stretched defences.

The threat posed by fraud is profound and complex, and can undermine every aspect of an organisation from staff morale to customer confidence, from the brand to the balance sheet. The response it deserves should not be fragmented, piecemeal and *ad hoc*, but sustained, certain and integrated.

To defend against fraud in a holistic way, and to meet the fraud governance expectations of *all* stakeholders, organisations need to raise their heads to survey the commercial environment as it really is, in all its complexity and confusion, and to tackle fraud risk factors wherever they are found.

Self-help

Society's existing fraud defences have never been resourced to match the true scale of the fraud threat, but now they are weakened further by cuts in public services, including law enforcement, and by renewed political uncertainty. The future of almost every element in our system of regulation, investigation and prosecution is in question. We face a future with 22% fewer police officers. How many fraud squads will escape the axe for much longer? The SFO has recently lost another cohort of senior and experienced staff and had its budget cut by a quarter. At the same time its operational focus on bribery and corruption has further reduced the resources available to tackle other types of serious fraud.

The landscape of anti-fraud legislation and regulation is changing fast: even as cost cutting slashes budgets across the criminal justice system, much more change is promised. This is a time of upheaval in which organisations would be wise to make the most of *self* defence, and to avoid weakening it in the rush to cut costs.

The Fraud Advisory Panel's fraud factsheets can play a vital role in helping organisations do this.

Taking charge
an action plan for business

How a company manages its fraud risks is a vital part of good corporate governance. Governance failures – and especially those in which fraud and dishonesty play a part – can cause lasting damage to corporate reputation and value. That's why the governance of fraud risk management is increasingly seen as a proxy measure for commitment to wider society and long-term competitive fitness.

A proportionate response

Wise organisations create anti-fraud defences that are proportionate to the risks they face and appropriate to their size and circumstances. But what does this really mean in our modern world of instant communications, globalised ethical expectations and dynamic, technology-driven fraud threats?

Approaches to detection and prevention need to match the dynamism, imagination and flexibility of the fraudster. This means building fraud resilience into every aspect of an organisation's operations; harnessing hard and soft controls, engaging staff and management at every level, reaching down through the supply chain and out to the very front line of the customer experience, to build a truly fraud-intolerant culture from top to bottom.

Understanding your fraud risk

Before an organisation can do any of this, it must be clear about what it means when it talks about fraud and dishonesty in the specific context of its own business. Previous research has found that organisations that under-invest in anti-fraud systems suffer relatively high levels of fraud losses. But it is impossible to invest in a properly calibrated fraud risk management infrastructure without a clear understanding of the risks you face. How many organisations have made a real effort to define their true fraud risk 'appetite', and to really get to know what it is they may have to swallow when the worst happens?

So many fraud risks are so well camouflaged that in reality it can be very hard to get anything like an accurate understanding of threat. Increasingly there are large overlaps between the risks arising from cybercrime, bribery and corruption, money laundering and fraud. Legal definitions are just a starting point. Some forms of unethical behaviour – something as simple as turning a blind eye to the criminality of others – may not amount to criminal conduct but can be very damaging indeed, especially in the long-run. In some cases – bribery, for example – the law and ethical considerations coincide. In others – such as greenwash* – they surely will.

* Greenwash is the deceptive use of green ideas and imagery in PR or marketing to promote a misleading impression that a company's policies or products are environmentally friendly.

Be imaginative

We need to exercise imagination and be creative in seeking out vulnerabilities and loopholes, and in calculating likelihood and consequences.

Try to look afresh at well-established and familiar processes, practices and relationships as if you are standing in a criminal's shoes! What weaknesses would a fraudster see hidden amid the workaday routine? Are there places in which familiarity has tipped over into complacency? Have new vulnerabilities been opened up by changes in legislation, regulation, reporting standards, IT infrastructure or relationships with strategic suppliers?

Bitter experience shows that when organisations think they have low fraud risks they have often been looking for them in the wrong places. What's obvious to the criminal mind may be almost literally invisible to anyone else. But fraud-fighters know that most frauds are old songs played on new instruments (often the internet), so we must train managers and staff to recognise and understand real-life fraud techniques, then ask them concrete questions about risk based on this new understanding.

Be brave

Have the courage to consider worst-case scenarios too. We do the fraudsters' work for them when we deceive ourselves about the true costs of the risks we run. Most importantly, include the threat from wrong-doing at the highest levels of management. Too many senior executives still think that fraud risk management controls are for other people. Very few organisations profile the risk of corrupt leadership, even though fraud is often a crime of the powerful. Consider the cost to stakeholders of a company saddled with a disastrous acquisition strategy designed by a corrupt CEO and CFO to enrich only themselves. The KPMG fraud barometer found management fraud had increased by 20% in 2010, costing £419 million or more than three times the £129 million of fraud committed by employees. And yet still it's the junior accountant with a drug habit that we plan for!

What's wrong?

Efficient fraud risk management is founded on prevention, and staff are its corner stone. They need to know what a red flag looks like if they are to recognise one when they see it. But nor should we leave to chance staff understanding of what is and is not appropriate personal behaviour.

Ethical cultures thrive on clarity and certainty. Anti-fraud communication and training programmes must go well beyond generalisations, providing employees with clear guidance and specific examples of what is, and is not, ethical.

And take a zero tolerance approach to dishonesty. Where unethical business behaviour of any kind is tolerated or condoned there is the risk of poisoning the wider culture and emboldening insiders to bite the hand that feeds. Conversely, a strong organisational culture, one that sets high ethical expectations for all, can influence for the better the behaviour of anyone who might be vulnerable to committing or tolerating a crime.

Who owns fraud?

Good governance means not just senior level ownership of the organisation's anti-fraud defences, but hands-on involvement too. Anti-fraud strategy should be a board level responsibility.

Boards should take an active interest in the incidence of fraud, receiving regular reports and making sure they are being kept fully informed of major events. But this raises some tough questions about what it is they should be looking at. To be useful, fraud data need to be accurate, detailed and recognisable. Nor should they be made invisible by statistical aggregation or euphemism. A fraud is not the same thing as a 'bad debt', an 'insured loss', or 'shrinkage'.

Then there's the data reported to senior management in such areas as health and safety, greenhouse gas emissions or toxic waste disposal. How reliable and representative are these? They matter increasingly to corporate value through the harm (or good) they do to an organisation's reputation for social and environmental responsibility and sound long-term stewardship.

(Consistent) tone from the top

Surveying its Fraud Academy membership, PwC found that the vast majority believe that strong ethical leadership, coming straight from the chief executive or the head of finance, is crucial in mitigating fraud risk. The Bribery Act 2010 is very clear on the importance of tone from the top in establishing and guiding ethical behaviour throughout an organisation. But to be effective, ethical leaders also need to be consistent and visibly so. Ethical cultures are not built on double standards.

And don't forget the middle managers. They are closest to the front-line, where operational decisions and ethical judgements are made minute-by-minute. The whole-hearted commitment of middle management is a pre-requisite of long-term change. Without it, and without sustained senior level sponsorship, a sincerely held desire to build an ethical culture may turn out to be little more than a flurry of short-term initiatives.

"Those at the top of an organisation are in the best position to foster a culture of integrity where bribery is unacceptable."

Principle 2, paragraph 2.1 of guidance published by the Ministry of Justice under Section 9 of the Bribery Act 2010

Speak up!

Formal, secure and trusted whistleblowing or 'speak-up' procedures stopped being an optional extra some time ago. They are good for business and good for reputation, but in particular they are good for morale. Since 1999 the employee protections created by the Public Interest Disclosure Act have meant that organisations without effective whistleblowing procedures risk leaving concerned employees with no alternative but to voice those concerns publicly.

A planned response

A key part of fraud-fighting preparedness is the creation of a fraud response plan. Heightened awareness among staff and management will result in the discovery of more dishonesty and fraud, inside and out. A formal fraud response plan – outlining the who, what, when and how of investigation, reporting, discipline and post-mortem – reduces the heavy resource cost of fire-fighting, and clearly demonstrates the organisation's commitment to tackling fraud head on. It can also benefit morale by ensuring that everyone knows what to expect, and what will be expected of them, if a fraud is discovered or suspected and an investigation is launched.

Fraud reporting: a shared responsibility

In September 2010 the Panel published its detailed review of the present architecture for reporting corporate fraud among listed companies. Is it, we asked, adequate, coherent and fit for purpose? The answer that emerged was not encouraging.

The UK is now dependent on a patchwork of reporting obligations with a worrying absence of any common thread. Those obligations that do exist are disparate and difficult to discern, often flowing implicitly from broad principles of law or professional regulation, rather than being comprehensive and coherent, rooted in explicit statements of practice or prescription.

Although the case for change is compelling, companies remain reluctant to report fraud to external parties, particularly the police, for a host of well-documented reasons. These reasons vary widely in quality and plausibility, but even the best provides no persuasive response to two pressing realities:

- widespread corporate fraud is hugely damaging to individual businesses and a corrosive threat to society;
- a more synergistic and consistent approach to reporting would vastly improve progress in reducing the incidence of corporate fraud in the UK.

Responsibility for fraud prevention and detection does not and should not rest with the board of directors alone. It should be a widely-shared responsibility under which directors set policy and 'tone', senior management (including internal audit) implement and ensure compliance, and employees adhere and report concerns.

Full report and a summary from:
www.fraudadvisorypanel.org/new/publications

Fraud Advisory Panel
Chartered Accountants' Hall
PO Box 433
Moorgate Place
London, EC2P 2BJ

Tel: 020 7920 8721
info@fraudadvisorypanel.org
www.fraudadvisorypanel.org

Registered Charity No. 1108863