Identifying and Responding to Corporate Fraud in the 21st Century

Australian Institute of Management

Sydney

20 March 2002

Adam Graycar
and
Russell Smith

Australian Institute of Criminology
GPO Box 2944, Canberra 2601
phone: 02 6260 9205
fax: 02 6260 9203
e-mail: adam.graycar@aic.gov.au
russell.smith@aic.gov.au

Fraud involves the use of dishonest or deceitful conduct in order to obtain some unjust advantage over someone else. Fraud currently costs the community in excess of $3.5 billion, and last year alone cost the Commonwealth Government over $150 million. It costs big business megabucks, though the dollar value is hard to ascertain. Its not just big business and government - at the Australian Institute of Criminology we are ready to release data from a study of crime against small business, which shows that fraud costs small business more in dollar terms than employee theft, burglary, armed robbery, unarmed robbery, and vandalism.

The prevention and control of fraud are two of the great challenges for Australia now, and in years to come.

It has been around for as long as people have been around - somebody trying to con somebody else, to offer them an unbelievable and unattainable deal, or to work the system unlawfully to their own advantage so that things come incredibly easily. While crimes of deception are well-established in history, technological, social, demographic and economic developments have brought about changes in the form fraud takes and how it is perpetrated.

The circumstances in which fraud can exist are enormously diverse. Some of the types include: commercial fraud, fraud against governments, consumer fraud, migration fraud, securities fraud, superannuation fraud, intellectual property fraud, computer and telecommunications fraud, insurance fraud, plastic card fraud, art fraud, charitable contribution fraud, identity-related fraud, advance fee fraud, health care fraud, the list goes on and on, and new opportunities for deceptive conduct arise all the time.

The basic motivation for fraud is greed, a fairly robust and enduring human characteristic. We are unlikely to eliminate greed in my lifetime or yours, so countermeasures have to be more than psychological or feelgood tactics.

Crime follows opportunity, and opportunities for fraud flow from economic growth. The more commerce there is, the more opportunities there are to commit fraud. Nobody wants to pull the plug on electronic commerce, close down the stock market, or the health insurance system, just because they may be vulnerable to fraud.

Rather, the challenge lies in designing systems which allow commerce to flourish while blocking opportunities for fraud. This challenges us to extend our ingenuity to counter that of villains, and to build smart systems.

Like all crimes, fraud is the product of 3 factors

- Motivation - somebody willing to offend
- The presence of a prospective victim or target
- The absence of a capable guardian

This general rule applies whether we are referring to fraud against a government benefits program, fraud against elderly people, fraud against your organisation, or misappropriation of corporate assets by a company Director.

Three ways to work on the limitation of fraud involve:

- Reducing the supply of motivated offenders
- Protecting and educating the suitable targets
- Limiting opportunities by making the crime more difficult to commit

I am not going, this morning, to be able to go through the whole gamut of fraud, so I'll focus only on 4 types of examples: *Telecommunications Crime; Electronic Funds Transfer Crime; Identity-Related Crime; On-line Sharemarket Manipulation.*

While fraud has been around forever, the common thread running through most of the current wave of economic crimes is that they are greatly facilitated by recent developments in information technology.

The convergence of computing and communications technologies has changed dramatically the nature of corporate life. Digital technologies are present throughout all aspects of business activity—

- new companies are able to be registered and official documents lodged with regulators electronically;
- Information required to be given by financial advisers to their clients (such as Product Disclosure Statements under the Financial Services Reform Act 2001, which came into effect last week) can be given electronically;
- business records are able to be maintained electronically and archived on computerised databases;
- GST compliance documents are able to be submitted electronically (and indeed if your company has an annual turnover of more than $20 million, must be submitted electronically);
- many Stock Exchanges now offer electronic trading systems from dedicated terminals which enable securities to be bought and sold on-line; and
- personnel matters are able to be carried out electronically such as through the use of video-conferencing for job interviews, analysing working patterns though the use of neural networks, and paying staff electronically through the use of electronic funds transfers.

The benefits of computing and communications technologies are clearly apparent.

People are able to communicate more effectively and at lower cost than in the past. It has also meant that geographical boundaries are able to be crossed more easily which has enhanced the process of globalisation of economic and social life enormously.

These same technologies that have provided so many benefits have, however, created enormous opportunities for offenders—

Criminals are able:

- to communicate with each other in secret,
- to disguise their identities in order to avoid detection, and
- to manipulate electronic payment systems to obtain funds illegally.

They are also able to perpetrate fraud on a much wider scale than in the past, duplicating countless fraudulent invoices, or establishing large numbers of accounts that only exist in cyberspace. Their victims may also be located anywhere in the world.

Finally, the potential losses that could be sustained through electronic corporate fraud are enormous—a fact which many enterprising and technologically literate offenders know only too well. The extent to which individuals are using the Internet for business transactions has, for example, increased dramatically. In terms of commercial usage, Forrester Research has estimated that global business-to-business electronic commerce will be worth US$2.7 trillion by 2004 while the Gartner Group puts this figure closer to US$7 trillion. If even a small fraction of this is lost to fraud, substantial sums will be involved.

Telecommunications Crime

In the old days phone fraud meant putting a metal washer into a pay phone to make a "free" call. Now, telecommunications systems can be manipulated to perpetrate crime. One of the great weaknesses in the past has been PABXs which have been manipulated so as to enable long-distance telephone calls to be charged to organisations without authorisation. Sometimes substantial sums have been involved. In the United Kingdom, for example, a case of PABX fraud cost a government department the equivalent of US$80,000 a day while another department lost US$640,000 over a six week period. In yet another case, illegal access was gained to Scotland Yard's PABX system in London by computer hackers based in the United States. Unauthorised international calls to the value of A$1.29 million were made for which Scotland Yard was liable. Other cases have involved tee-ing into telephone lines and cloning of mobile telephones, many of which have involved employees within organisations disclosing confidential security information to enable the crime to be committed.

In a case reported to the Australian Federal Police in 2001, hackers gained access to computer switchboards of twelve of Australia's largest corporations and incurred A$12 million worth of untraceable phone calls. Have you taken precautions to ensure the integrity of your phone system?

Electronic Funds Transfer Crime

All companies and organisations move money electronically. In the old days you would stand in line in a bank and hand a piece of paper over to a teller who probably

knew you by sight, and if there was an anomaly in your ledger, it would be picked up by a bank official who just knew!

Crime today takes place by manipulating the security systems established to protect electronic funds transfers. These systems are designed to ensure that information cannot be manipulated as it passes over computerised networks and that only authorised users have access to computers.

Most of the large scale electronic funds transfer frauds which have been committed in the past have involved the interception or alteration of electronic data messages transmitted from the computers of financial institutions.
In many cases offenders have worked within financial institutions or corporations themselves and been privy to the operation of the security systems in question.

One recent example of funds transfer fraud involved a financial consultant contracted to the Department of Finance and Administration in Canberra who, on 25 September 2001 was convicted of defrauding the Commonwealth by transferring A$8,735,692 electronically to private companies in which he held an interest. He did this by logging on to the Department's computer network using another person's name and password. He also was able to obscure an audit trial by the use of other employees' logon codes and passwords. He was sentenced in the ACT Supreme Court to 7 ½ years imprisonment.

Could this sort of thing happen in your organisation?

Identity-Related Crime

In the old days bushrangers and outlaws used masks to cover their faces so nobody would know who they are. Today, on the internet, nobody really knows who you are.

One of the most frequently used strategies to perpetrate crime is the creation of false documents used to misrepresent one's identity. Once a convincing identity has been fraudulently established, it is then possible to defraud organisations, steal funds and then to evade detection, investigation, and arrest. Australian police services have recently found an increase in such misrepresentations which have been used for money laundering and tax evasion, to obtain personal loans from banks, enter into hire-purchase agreements, and deal in stolen motor vehicles. Often counterfeit documents have been created by a single person to support multiple identities, each being used once only for a specific illegal enterprise, and then discarded.

In my Identity Fraud talk, (which is not today's talk!) I go through a case a man recently convicted in Melbourne for manipulating identities, opening accounts, forging documents to obtain drivers licences, moving money which was not his, establishing companies, setting up payrolls, getting tax returns - he made half a million dollars fairly easily. But he got caught! There is another case we use in which a Japanese man used the Internet to advertise the availability of bank accounts he had

opened using false identities. He allegedly sold the bank accounts through the Internet to enable his customers to use the accounts to perpetrate fraud and other crimes

The technology of the Internet makes it relatively simple for users to disguise their identities. Electronic mail and Internet addresses may be manipulated by including details which are misleading or the source of a message may be made anonymous or changed so that it appears to be coming from another user. Similarly, there is no way of knowing the commercial affiliations of those on the Internet. Referees for businesses or products might, in fact, be individuals employed specifically to indicate their approval of the venture or product in question.

Businesses might also choose legitimate-sounding names in order to improve their credibility or include domain names which are misleading. There has recently developed a practice in the United States and Canada of some businesses adopting domain names containing the names of Australian cities in order to improve their marketability and credibility, despite the fact that they have no connection at all with Australia.

In one case investigated by the ACCC, an Internet trader used the same domain name as another trader (the original bearer of the name), but with a <.com> suffix, as opposed to the <.net> suffix of the original site. The confusion created as to the identity of the actual proprietor of the site allowed consumers to be misled or deceived. The <.com> site did, however, include an inconspicuous notice stating that the site should not be confused with the <.net> site of the same name, although this could easily have been overlooked by those visiting the site.

On-line Sharemarket Manipulation

The use of computers and E-mail has greatly facilitated the manipulation of sharemarkets during secondary trading of securities. This can occur through the use of rumour, hyperbole, or other forms of misinformation to boost the price of a stock prior to the manipulator's quick and profitable exit ('pump and dump'), or by talks down a stock so that he or she may buy in at a bargain price ('slur and slurp').

In a recent Australian prosecution, a 24 year-old man who lived in a Melbourne suburb, manipulated the share price of an American company by posting information on the Internet and sending E-mail messages around the globe that contained false and misleading information about the company. On 8 and 9 May 1999, he posted messages on Internet Bulletin Boards in the United States and sent more than four million unsolicited E-mail messages to recipients in the United States, Australia and in other parts of the world. The messages contained a statement that share value of the company would increase from the then current price of US$0.33 to US$3.00 once pending patents were released by the company, and that the price would increase up to 900 per cent within the next few months. The effect of the information was that the company's share price on the NASDAQ doubled, with trading volume increasing by more than ten times the previous month's average trading volume.

The offender had purchased 65,500 shares in the company through a stock broking firm in Canada several days before he transmitted the information. He sold the shares on the first trading day after the transmission of the information and realised a profit of approximately A$17,000. The offender was prosecuted by the Australian Securities and Investments Commission for distributing false and misleading information with the intention of inducing investors to purchase the company's stock. He pleaded guilty and was sentenced to two years' imprisonment on each of three counts, to be served concurrently. The Court ordered that twenty-one months of the sentence be suspended upon his entering into a two-year good behaviour bond with a surety of $500.

These are only some of the types of fraud facing Australian organisations today. Before discussing what to do about it, you have to know that you're being scammed. This is not nearly as obvious as it sounds, and often does not come to light until late in the piece - often too late! There are certainly some risk factors, and some red flags.

Always look for anomalies - in essence, there are three types of anomalies to look out for, behavioural anomalies, statistical anomalies and organisational anomalies.

Behavioural anomalies can be found in people suddenly changing their lifestyles, living beyond their means - they might have come into a lot of money legitimately, but keep an eye out for behavioural anomalies.

Statistical anomalies are when the numbers don't look right, expenses claims out of whack with past patterns, sudden changes in credit card bills, tax deductions out of proportion to income, insurance claims that bear no resemblance to a person's lifestyles etc.

Organisational anomalies are activities which diverge notably from best practice - inadequate systems of communication within the organisation, lack of transparency to outside observers, the absence of financial control systems, the Board of Directors handpicked by the CEO., poor leadership, inflated financial targets, unrealistic incentive structures based on commissions are all risk signals.

The absence of anomalies, however, does not mean the absence of fraud. How, then should corporations respond to these risks? Some of the solutions simply involve the application of conventional risk management strategies while others entail the adoption of new technological approaches, or reliance on traditional legal responses. There are, however, a number of challenges that managers face in responding to corporate fraud in the twenty-first century.

You will remember that at the outset, I said the three main preventive strategies were to

- Reduce the supply of motivated offenders
- Protect and educate the suitable targets

- Limit opportunities by making the crime more difficult to commit

Let me outline four general preventive strategies:

- Effective Corporate Governance
- Fraud Control Policies
- Personnel Monitoring
- Computer Usage Monitoring

These however are a backdrop to the hard approach - using a range of technologies to prevent corporate fraud, or using the criminal justice system to prosecute and punish offenders.

Very briefly, the technologies involve a range of hardware security measures, the use of access controls which use passwords or smartcard tokens; the protection of computer cables from interception when digital signatures and encrypted data transmissions take place, and other digital signature security measures; a range of card security measures; user authentication; biometrics; fraud detection software (neural networks), etc.

The use of legal prosecution and punishment is one of the principal means of deterring criminal conduct in both digital and non-digital environments. Although the process may be time consuming and costly, the publicity which a criminal conviction and sentence of imprisonment attracts can be beneficial in terms of ensuring that potential offenders take the consequences of acting illegally seriously.

The extent to which lengthy terms of imprisonment constitute a deterrent to criminal conduct is, however, open to debate. Whilst many property offenders behave more or less impulsively, computer criminals are relatively more likely to engage in rational calculation, making some assessment of the prospective benefits and costs of a given fraudulent course of action. In these circumstances, the greater the perceived likelihood of conviction and the more severe the expected punishment, the less the inclination to offend.

Prison, however is not a panacea. But that's another story

Ideally, business culture and ethical behaviour is the start - with the catalogue of issues I mentioned a moment ago.

Effective Corporate Governance

In the first place it is important for those who manage companies to have a proper understanding of the risks that are present within their organisation. This requires managers to know precisely how their business operates. Often those in charge of companies may not understand how their organisations function in sufficient detail to

be fully aware of the risks of fraud that exist. This is particularly the case with respect to information technologies. In Ernst and Young's survey of large organisations, for example, less than one third of the Australian respondents considered that their directors had a good overall understanding of their business for fraud prevention purposes.

Although managers may not be able to understand the technicalities of all the computer software and hardware that their organisation makes use of, they should be in a position to understand the areas where fraud risks arise and instruct appropriately trained personnel to monitor these areas regularly.

Fraud Control Policies

It is also important for organisations to have clear and transparent fraud control policies in place. These are necessary in the digital environment no less so than in the terrestrial world.

Australian Standard No. AS 3806-98 *Compliance Programs* provides guidelines for both private and public sector organisations on the establishment, implementation and management of effective compliance programs. The Standard also provides principles which organisations are able to use to identify and to remedy any deficiencies in their compliance with laws, industry codes and in-house company standards, and to develop processes for continuous improvement in risk management.

Establishing principles on, for example, the ethical use of information technologies and how to respond to instances of fraud are essential in conducting a business of any kind, whether or not it makes use of electronic commerce.

Of particular importance is the need to develop specific policies on computer security along with appropriate guidelines on reporting computer misuse and abuse. Policies need to deal with specific on-line behaviour of employees such as security of user authentication systems (e.g. passwords), access to and use of the computers for private purposes, personal use of electronic mail, downloading software, and the use of copyright material. Principles also need to be established to ensure that those who report illegal conduct are not disadvantaged by their conduct.

Personnel Monitoring

There is also a need for organisations to be confident that the staff they are employing are reliable and trustworthy, as electronic fraud often involves confederates with inside knowledge of a company's security and computer procedures. The administration of modern technologically-based security systems involves a wide range of personnel—from those engaged in the manufacture of security devices to those who maintain sensitive information concerning passwords and account records. Each has the ability to make use of confidential information or facilities to commit fraud or, what is more likely to occur, to collude with people outside the organisation to perpetrate an offence.

Preventing such activities requires an application of effective risk management procedures which extend from pre-employment screening of staff to regular monitoring of the workplace.
Long-term employees who have acquired considerable knowledge of an organisation's security procedures should be particularly monitored, as it is they who have the greatest knowledge of the opportunities for fraud which exist and the influence to carry them out.

Caution is also needed when internal disputes develop.

A case heard before the New South Wales District Court on 27 March 1998, for example, concerned an unsuccessful applicant for a position with an Internet Service Provider (ISP). When he was refused the job he took revenge by illegally obtaining access to the company's database of credit card holders and publishing details relating to 1,225 cardholders on the Internet as a demonstration of the security weaknesses of the company. As a result, the business lost more than $A2 million and was forced to close its ISP activities.

Computer Usage Monitoring

Employees' use of computers and their on-line activities can be monitored through the use of software which logs usage and allows managers to know, for example, whether staff have been using the Internet for non-work-related activities. Ideally, agreed procedures and rules should be established which enable staff to know precisely the extent to which computers are able to be used for private activities, if at all. If staff are permitted to make use of computers for private purposes, then procedures should be in place to protect privacy and confidentiality of communications, subject, of course, to employees obeying the law.

Where certain on-line activities have been prohibited, it is possible to monitor the activities of staff, sometimes covertly such as through video surveillance or checking electronic mail and files transmitted through servers.

Filtering software may also be used to prevent staff from engaging in certain behaviours. 'Surfwatch', for example, can be customised to deny employees access to specified content. When the employee requests a site, the software matches the user's ID with the content allowable for the assigned category, then either loads the requested page, or advises the user that the request has been denied. The software also logs denied requests for later inspection by management.

The use of computer software to monitor business activities also provides an effective means of detecting fraud and deterring individuals from acting illegally.

The Consequences of Failure to Respond to Fraud within Organisations

Where corporations have experienced electronic fraud, managers are faced with difficult choices as to how they should respond. On the one hand, they may choose to

'exit' the situation — and to dismiss the employee responsible, or cease doing business with the individual who perpetrated the offence.

On the other hand, they may seek legal avenues of redress, either employing civil proceedings to recover compensation or criminal proceedings to punish the offender and to deter others from acting similarly.

Many organisations prefer not to report crime to the authorities. A survey of organisations victimised through fraud conducted by Deakin University found that fraud was not reported officially because the matter was not considered to be serious enough to warrant police attention, a fear of consumer backlash, bad publicity, inadequate proof, and a reluctance to devote time and resources to prosecuting the matter.

The reasons for the reluctance to report fraud are often due to a fear of 'sending good money after bad' as experience may have shown that it will be impossible to recover losses successfully through legal avenues and that the time and resources which are required to report an incident officially and to assist in its prosecution simply do not justify the likely financial returns. Prosecution may entail countless interviews with the police, extensive analysis of financial records, and lengthy involvement in court hearings for staff.

The other disincentive to taking official action lies in the reluctance of organisations to publicise the fact of their victimisation through fear of losing business or damaging their commercial reputation in the marketplace. Government agencies might also believe that adverse publicity may result in a loss of confidence in voters, whilst financial institutions might believe that publicity of security weaknesses might result in acts of repeat victimisation taking place using the same techniques as those being investigated.

Finally, where crime has been committed by those in positions of responsibility within organisations, they may not wish to draw undue attention to their own illegal activities.

Although some of these responses are understandable, failure to take action creates an undesirable atmosphere in the organisation indicating that fraud is tolerated. It may also may result in the offender in question being able to reoffend, either in the same organisation or elsewhere. Failure to report crime also means that new forms of crime do not receive publicity and thus others may be victimised in the same way. Finally, if crime is not reported then it is not possible to gather statistics on the nature and extent of incidents that takes place.

There are no easy fixes!

Conclusions

Fraud is not going to go away. The electronic systems used to conduct commercial transactions are changing rapidly, and considerable effort is being put into ensuring the security of digital transmissions which represent monetary value. The opportunities for fraud are, however, substantial.

The solution to corporate fraud will ultimately involve the adoption of a range of strategies both technological and strategic in which close cooperation will exist between all those involved in providing and using systems. This includes telecommunications carriers and service providers, financial institutions, corporations, and individual users.

Going back to my three opening points, reducing fraud involves

- Reducing the supply of motivated offenders
- Protecting and educating the suitable targets
- Limiting opportunities by making the crime more difficult to commit

⇒ To deal with the first objective, reducing the supply of motivated offenders, is a hard one because there has always been greed, and the traditional crime prevention activities of early intervention are not applicable. People commit fraud without many of the usual risk or predictive factors. We are dealing here with culture and ethics - not something that comes in a five minute pep talk It is here that things like effective corporate governance and ethical standards are central. At the other end of the spectrum, but dealing with the same issue of reducing the supply of motivated offenders, judicial punishments also play a role. Prison, which has few redeeming features, probably works better as a deterrent for fraud offenders than for many others. Similarly, confiscating a fraudster's home or car and requiring ill-gotten gains to be repaid over a lifetime are appropriate sanctions for white collar offenders.

⇒ To deal with the second objective, protecting and educating the targets of fraud is a crucial part of the prevention equation. It involves a knowledgeable and informed public able to identify an offer which appears "too good to be true" as well as a mechanism for keeping new information flowing, at both an individual and organisational level. This goes hand in hand with a fraud control policy.

⇒ Limiting opportunities by making the crime more difficult to commit brings in the other side of the prevention equation, f control policies, computer usage monitoring, policing anomalies, corporate governance and professional regulatory procedures. The technologies of crime prevention are also of fundamental importance here.

It all points to careful risk management. Risk management and fraud prevention are clearly preferable to the use of prosecution and punishment.

The prevention and control of fraud are two of the great challenges for Australia in the years to come. Success in dealing with fraud will enhance Australia's business

reputation, and reduce the personal hardship that fraud causes to countless victims each year.

Most fraud in the twenty-first century is sophisticated in planning and execution. Fraud prevention also needs to be sophisticated, although, as a recent British Home Office publication notes, it's 'Not Rocket Science'! Some aspects of fraud prevention may involve individuals in the community taking basic measures to protect themselves, such as by using the security measures that modern computing technologies have to offer in a sensible and thoughtful way—and not simply writing one's password on one's deskpad! Other target hardening measures may require elaborate and complex planning in order to thwart the efforts of fraudsters fully trained in the operation and management of electronic business systems.

Managers also need to take personal responsibility for dealing with fraud and for reporting it to the authorities. This will not only help to inculcate an environment of honesty and openness within an organisation, but will enhance deterrent effects for other staff and enable the public generally to understand new areas of risk and security weaknesses. Sweeping fraud under the carpet by dismissing untrustworthy employees, compounds the problem and creates an atmosphere of complacency within organisations. At every available opportunity, a **culture of compliance** needs to be reinforced.

In the end, fraud prevention and control require the concerted efforts of individuals working both within the public and private sectors who make use of the most up-to-date and effective fraud control technologies. When all else fails, an efficient legal system must also exist to detect, investigate, adjudicate, and sanction those who seek to obtain funds dishonestly. There has been considerable progress in each of these aspects already and Australia is at the forefront of many innovative developments in fraud control.

The challenge for the years to come lies in understanding how new forms of fraud are perpetrated and ensuring that those charged with preventing and dealing with fraud have adequate resources to do their work. As in most areas of crime control, it is better to allocate resources in preventing crime than in seeking to deal with the consequences after the problem has arisen.