14th Annual Conference of the Australian
and New Zealand Society of Criminology

***The Future and Criminology: New Solutions for Old Problems
or Old Solutions for New Problems?***

University of Western Australia
30 September 1999

"Defrauding Governments in the Twenty-First Century"

Russell G. Smith
Australian Institute of Criminology

Introduction

Governments throughout the developed world have found that considerable benefits can be derived from delivering services electronically. Not only are people able to respond to official requests for information via computers, but they can request the payment of benefits and receive funds by way of electronic transfers made directly to their bank accounts. In addition, digital technologies play a critical role in the daily activities of public servants be they clerks, researchers, or politicians. This paper examines how these developments are able to be put to improper use and how the growing use of computer technologies by government agencies will create additional risks of illegal and fraudulent conduct in the future. A variety of solutions to the problem, many of which also make use of computers, will also be described.

Throughout history attempts have been made, often successfully, to defraud governments by stealing money, misappropriating government property, misusing time, or stealing information. The scale of such crime varies from the trivial, such as having an extended lunch break, to the serious, such as large-scale revenue fraud. In KPMGs most recent fraud survey, some sixty-two per cent of the thirty-nine government organisations surveyed had experienced fraud in the preceding two years (KPMG 1999).

Some of the largest losses which governments have sustained relate to the evasion of payments due to them, such as taxes and fees, and obtaining benefits to which the recipient is not entitled such as welfare benefits and educational and travel allowances. Government employees have also

stolen funds and other government property both directly and indirectly. Direct theft may occur when employees steal petty cash or remove government property. More covert forms of theft involve the abuse of government facilities such as the use of motor vehicles and computers for non-government use. Government employees are also well-placed to abuse their position by accepting bribes to grant licences for which there is no entitlement or to charge governments for goods or services which are not in fact provided.

In recent years, the use of computer technologies by governments has increased enormously and the future will see many government services being provided through the use of on-line facilities. In the United Kingdom, for example, the government expects twenty-five per cent of all government services to be available electronically by 2002 (http://www.number-10.gov.uk/public/info/releases/publications/infoagefeat.htm), whilst in Australia the Commonwealth government has determined to provide all appropriate government services online by 2001 (http://www.law.gov.au/aghome/agnews/1998newsag/478a_98.htm).

The Commonwealth government has developed a strategy, Project Gatekeeper, which seeks to provide a system of secure electronic communications on public networks when dealing with the government through the use of public key cryptography and digital signatures (Office of Government Information Technology 1998). In Victoria, an on-line government service known as 'Maxi' has been created which enables members of the community to gain access to Victorian government and certain private sector services through telephone, the Internet and at community kiosks (http://maxi.com.au). 'Service New South Wales' provides a similar service whilst in the Australian Capital Territory, individuals are able to obtain government and community information and pay certain bills at 'Austouch' kiosks (http://www.act.gov.au/austouch/austouch.html). The use of such technologies will undoubtedly enhance the efficiency with which governments discharge their responsibilities to the communities they serve.

The possibility, exists, however, that dishonest individuals might seek to misuse computers to defraud governments or otherwise to steal from them. Already this is taking place. In a survey of computer crime and security conducted by the Office of Strategic Crime Assessments and the Victoria Police Computer Crime Investigation Squad (1997: 30), thirty-six per cent of the eleven government agencies surveyed reported misuse of

their computer systems with forty-five per cent reporting external forms of attack, that is remote access to computer systems. The most frequently reported types of computer abuse reported by the government agencies surveyed related to damage or unauthorised access to, or copying of data and programs. In Britain, a survey conducted by the Audit Commission of 5,500 public and private sector agencies in 1994, found that of the twenty-four government agencies which responded, forty-six per cent had experienced some form of computer abuse in the preceding three years. Of the sixty-six incidents reported, twenty-one involved fraud amounting to £678,874 in total (Audit Commission 1994).

The Nature and Extent of the Problem

How, then, are governments being victimised through the use of computerised technologies, and what opportunities exist for such technologies to be used for financial crime in the future? The vulnerabilities fall into five categories which are listed in order from those which involve the largest financial losses to those which involve the least : theft of benefits, money, information, computer hardware and software, and time. Although this arrangement in terms of importance is not based on empirical evidence, it does give some subjective indication of the areas of greatest concern.

Theft of Benefits

Revenue Fraud

Taxation departments throughout the developed world are now making extensive use of information technologies in the assessment and processing of private and business taxation liabilities. Already some taxation departments permit individuals to lodge taxation returns electronically and pay refunds through the use of electronic funds transfers. As global on-line commerce increases, the collection of revenue will be greatly facilitated through the use of computers, although the technologies adopted will create various risks. Most will relate to attempts to disguise transactions in order to avoid the payment of taxation, particularly consumption taxes levied against on-line transactions (see Bridges and Green 1998). In addition, attempts may be made to manipulate the payment of refunds or to increase entitlements to benefits. Such illegality may be facilitated where taxation office employees provide access to networks or conspire with outsiders to overcome security systems. Already there have been reports of taxation office employees having being involved in fraud and corruption. In Victoria, for example,

some 242 instances of illegality were reported between January 1994 to December 1997 (Hughes 1998).

Social Security and Health Benefits Fraud

As government benefits programs continue to be administered electronically, the opportunities for electronic fraud are also enhanced. One recent case involved a number of Centrelink employees who allegedly credited themselves with Electronic Benefit Transfer Cards using both legitimate and false identities in order to obtain illegal cash payments from the government (*AFP News* December 1998).

Misappropriation of funds from the Health Insurance Commission (HIC) is also an area of considerable risk by reason of the large sums of money processed electronically through the use of on-line claiming and payment systems. Between 1 July 1997 and 30 June 1998, 128,023 Medicare services amounting to $7,461,353 were processed by electronic funds transfer which, although a relatively small proportion of the 202.2 million Medicare services billed worth $6,334 million in the same year, will increase considerably in the future.

At present, the most common offences investigated by the Commission relate to claims for Medicare or Pharmaceutical benefits being made by means of false or misleading statements. In the year 1997-98, $7.6 million of benefits paid incorrectly were recovered or were in the process of being recovered from providers and the public. For the same year, a total of 2,812 complaints of alleged fraud and inappropriate practice were recorded on the HICs National Complaints Register (HIC *Annual Report 1997-98*, Professional Review Supplement, p. 17-18).
The HIC has already been subject to fraud perpetrated by insiders and the possibility exists that those with the technological skills could attack the Commission's electronic claiming system internally. In 1997, for example, two former HIC employees were convicted of defrauding the Commonwealth by creating false provider accounts and making illegal claims to the combined value of more than $45,000 (HIC *Annual Report 1996-97*, Professional Review Supplement, p. 23).

Credit Card Fraud

Government funds may also be misappropriated through the dishonest and unauthorised use of government credit cards. Providing government employees with credit cards is an efficient and secure way of paying for authorised goods and services as funds need not be drawn in cash which could be stolen prior to use. A survey undertaken by the Department of

Finance and Administration found that in the year to April 1998, there were 11,287 Australian Government Credit Cards in use which were used for 484,000 transactions with a total value of $162 million (Joyce 1999).

Transacting government business through the use of plastic credit cards, however, raises all of the security risks which cards bring with them (see Grabosky and Smith 1998, ch. 8). More importantly, however, is the possibility that government employees may use cards for unauthorised purposes.

In 1994, the Australian National Audit Office conducted an audit of a sample of transactions undertaken with the Australian Government Credit Card (Australian National Audit Office 1994). Since the card was introduced in November 1987 until March 1994, there were forty-six cases of fraud reported totalling between $1.8 million and $2.0 million for all departments and agencies. The bulk of cases related to claims under $5,000 with most of the frauds relating to the unauthorised purchase of goods to be used for private purposes or for travel and hospitality which had been paid for from other sources ('double dipping').

Despite widespread publicity concerning the risks of detection associated with improper use of official credit cards, government employees continue to abuse them often resulting in loss of employment and criminal prosecution when uncovered.

The Civil Aviation Safety Authority, for example, recently identified two cases in which its officers had abused Travel cards issued for official business. One individual had withdrawn his travel allowance from the Authority's bank and then used his Travelcard to pay for accommodation, meals, drinks, and in-house videos whilst on official business. Another officer used the Travelcard as a form of personal credit line by withdrawing cash and repaying it at a later time which was convenient (Joyce 1999).

Theft of Telecommunications Services

Government operations rely to a great extent on the use of telephones and, as such, fraud which is directed at telecommunications systems has the potential to inflict considerable losses on governments. There are innumerable ways in which to manipulate telecommunications systems in order to obtain services without having to pay for them (See Grabosky and Smith 1998, ch. 4), the most recent of which entail the use of digital technologies to compromise the security features of cellular telephones.

When carriers were wholly owned by governments, losses remained in the public sector. Now, such losses are largely sustained by private companies.

Government agencies and their staff, however, continue to make considerable use of telecommunications and occasionally they incur substantial losses through theft and fraud, particularly involving PABX technologies. In once recent case, for example, hackers based in the United States gained illegal access to Scotland Yard's PABX system in London by computer. Unauthorised international calls to the value of A$1.29 million were made for which Scotland Yard was held liable (Tendler and Nuttall 1996).

Misappropriation of Funds and Counterfeiting

Manipulation of computerised payment systems has been used for decades as a means of stealing from government agencies. An early case in the United States, for example, involved an employee of a welfare department who stole US$2.75 million over a nine month period by entering fraudulent data into the department's computerised payroll system. He then intercepted salary cheques sent to the 'phantom' employees, endorsed them to himself and cashed them. The fraud was uncovered when a police officer noticed some of the cheques in the offender's illegally-parked rental car (Brandt 1975).

The Australian Federal Police have also investigated a number of instances in which individuals have made use of Commonwealth computers to divert funds from government accounts. In one case, a programming contractor altered a government department's computer program so that funds would be automatically transferred to the individual's personal bank account (Baer 1996: 24).

In the Australian Capital Territory in 1998 a financial consultant to the Department of Finance and Administration allegedly transferred $8.725 million electronically to private companies in which he held an interest after logging-on to the Department's computer network using another person's name and password. (Campbell 1999).

Governments may also be victimised through acts of forgery and counterfeiting carried out through the use of desk-top publishing equipment (personal computers, scanners, and colour printers). Counterfeiting of currency issued by central banks has been greatly

facilitated through the use of electronic scanning equipment and colour photocopiers (Baer 1996). These technologies have also been used to forge government cheques, benefit claim forms, and payment vouchers along with primary and secondary documents used to establish false identities in connection with criminal activities.

Counterfeiting is, of course, not new. Daniel Perrismore, for example, was fined and pilloried for forging £100 notes in England in 1695 (Rastan 1996) and since then elaborate measures have been taken to improve the security of currency. Even Australia's polymer substrate currency, reputed to be one of the world's most secure (James 1995), and protected through the use of clear windows and holograms continues to be forged with convincing copies being produced electronically. In Western Australia, for example, in November 1998, four school students were allegedly involved in the counterfeiting of $50 notes through the use of computers, scanners and colour printers. (*AFP News* December 1998).

Theft of Information

The Australian Federal Police have also investigated cases in which unauthorised access has been gained to Commonwealth computers by employees, data illegally copied, and the copies sold to third parties (Baer 1996: 24). In South Australia, charges were laid against an employee of the Department of Social Security following the removal of a large quantity of records from the Department's database. Details of individuals held on the database were sold to a private investigator who sold them on to insurance companies (Australian Federal Police 1996: 20). In 1996, an employee of the Department of Social Security, a former police detective, was sentenced to 200 hours community service and fined $750 in Sydney after he was found guilty of unlawfully gaining access to and disclosing departmental information (Australian Federal Police 1997: 30).

Government employees have access to and make use of various forms of intellectual property in connection with their employment. Copyright, patents, trademarks, designs and certain other specific rights may all be used without authority. The greatest area of risk, however, lies in government-owned software being downloaded and used on personal computers for private purposes.

The possibility also exists that government employees may sell confidential, sensitive information obtained in the course of their employment. Although this has always been a risk, particularly in matters

involving national defence, the use of computers to discover information, such as through hacking, or to transmit information obtained illegally, makes the problem potentially much worse. In one case in 1997, an high-ranking agent working for the Central Intelligence Agency in the United States had attempted to locate sensitive information within the agency's computerised databases by carrying out searches for the keywords 'Russia' and 'Chechnya' and trying to gain access to databases without permission. Following an investigation, the FBI seized his computer notebook and found classified CIA documents on its hard drive and a floppy disk containing summary reports of CIA human assets. He admitted to selling top-secret intelligence information to the Russians for US$180,000 (Denning 1999: 133).

Theft of Computer Hardware and Software

Government employees are also in a position to steal computer equipment which often contains valuable software and sometimes sensitive information. In one recent investigation undertaken by the Australian Federal Police, a government department was the victim of a series of thefts of computers containing sensitive information. A number were recovered and three individuals charged. The department in question has since undertaken a review of its security and employee screening procedures to prevent similar incidents occurring (Australian Federal Police 1998: 43).

Laptop computers are particularly attractive targets for thieves, not only because of their portability, but also because of the information which they hold. One computer insurance company in Columbus, Ohio, received 309,000 claims in respect of stolen laptop computers and 100,000 claims in respect of desktop computers in 1997, worth US$1.3 billion in all. Where data held on hard drives are not backed-up, considerable inconvenience can arise from a theft. United Nations officials reported, for example, that the theft of four computers from its New York offices which contained data on human rights violations in Croatia, resulted in delays in the prosecution of war crimes from this region (Denning 1999: 157-8).

Theft of Time

Finally, one of the most difficult types of computerised theft from the government to detect is the theft of time (and, incidentally electricity) when employees use computers for unauthorised personal use at times when

they should be carrying out legitimate work. Although preventing this type of conduct could primarily be regarded as a matter of personnel management and workplace ethics rather than fraud control, in extreme cases unauthorised use of computers could result in serious disruption being caused to government operations.

Large-scale misuse of government resources in this way results not only in loss of productivity but also creates an inappropriate culture in the workplace and could, potentially, lead to problems of legal liability. The greatest area of vulnerability in recent times relates to inappropriate use of the Internet. Compaq Computer Corporation, for example, found in an analysis of the Web sites visited by its employees that twenty people had visited more than 1,000 sexually explicit sites each in less than a month. In a survey of executives conducted by *PC World*, twenty per cent of the 200 companies surveyed had disciplined staff for misusing Internet access with the most common offences involving visits to pornographic Web sites, shopping, using chat lines, gambling, and downloading illegal software (Denning 1999: 360-1). Although similar surveys have not been conducted of government employees' use of the Internet, it is likely that the same trends would be present.

In order to combat such problems, many government agencies monitor the activities of their employees, sometimes covertly such as through video surveillance or checking electronic mail and files transmitted through servers. Unauthorised use of the Internet has been checked through the use of filtering software or by employers publicising details of Web sites visited by their staff and naming the staff in question.

Legal and Law Enforcement Issues

Reliance upon the criminal justice system to deal with offences of dishonesty carried out electronically carries with it many complex legal and procedural issues. As a result, governments have generally focussed their efforts upon fraud prevention and the use of internal administrative remedies instead of proceeding to prosecution in the first instance. Large scale, and complex cases, however, usually result in criminal proceedings being brought in order to demonstrate publicly that fraud is taken seriously. In the realm of electronic commerce, it is also necessary to publicise the fact that novel forms of fraud can, and do, result in criminal sanctions being imposed.

There are, however, many impediments to mounting a prosecution. At the outset is the problem of identifying the illegal conduct in question and gathering sufficient evidence to discharge the burden of proof. Often police computer crime squads require the assistance of private sector forensic accountants or information technologists to ascertain and to analyse what transpired. Some offenders may have taken elaborate steps to disguise their identity or may have stored data on computers in encrypted form, thus making it difficult to decipher. The use of traditional search warrants might be impossible where police need to examine data on a hard disk in encrypted form where the offender is unwilling to cooperate. Laws may need to be amended in order to allow police to gain access to encryption keys so that incriminating records may be seized and presented to court in a readable form. Ensuring that data have not been tampered with also presents problems, although a document secured with a one-way hash function should overcome such concerns, subject to problems concerning the possibility that cryptographic keys and tokens had been compromised. The cost and time required to gather evidence may, however, make a prosecution practically impossible in all but the most important cases.

The criminal laws of many countries are, at present, inadequate to deal with prosecutions involving electronic transactions. Although a number of legal solutions are being devised to enable civil proceedings to be taken to enforce contracts made electronically, few countries have revised their criminal laws to permit electronic fraudsters to be dealt with.

One example of the type of problem which arises concerns the need to prove that the offender intended to carry out the proscribed conduct in question. Many offences against government authorities entail an element of deception or an element of intention to defraud and the question arises as to whether it would be possible to prove deception or intention to defraud where the conduct has been carried out against an electronic system as opposed to one conducted by human actors. At common law, deception entails the involvement of the human mind. It may be necessary to amend legislation to include an offence of 'causing a computer, machine or other device to respond to a false statement', such as exists in Australia's *Crimes Act* 1914 (Cth) s. 63(3) in relation to computer-generated forgery.

Fraud perpetrated against governments invariably involves the submission of false or misleading documents or forms or the making of false statements which may be made either orally or in writing. In a

dematerialised system, electronic documents and forms would be used and statements would be made electronically in the form of digital communications. It may be necessary to enact legislation which would ensure that offenders who have submitted false or misleading documents to governments electronically are able to be effectively prosecuted.

In Australia a Model Criminal Code has been proposed which would make a variety of changes to the law relating to fraud and forgery throughout Australia (see Australia, Model Criminal Code Officers Committee 1995). The definition of 'document' in clause 19.1(1) relating to forgery and offences involving false documents includes 'a disc, tape or other article from which sounds, images or messages are capable of being reproduced', while clause 19.1(2) provides that 'a reference to inducing a person to accept a false document as genuine includes a reference to causing a machine to respond to the document as if it were a genuine document'.

The Australian government has also developed an Electronic Transactions Bill 1999 which aims to provide an effective legal regime in which electronic commerce can be used. It provides that electronic communications should be treated in the same way for legal purposes as paper-based communications (functional equivalence). The proposed law, however, is primarily concerned with civil proceedings relating to the law of contracts and business transactions rather than criminal prosecutions and additional reforms would be needed to remove doubts as to the use of electronic data records in criminal trials.

The Council of Europe has also proposed guidelines for its member states to use when reforming their criminal laws to accommodate electronic transactions. Recommendations adopted include search and seizure of electronic data, surveillance of data transmissions, electronic evidence and the use of encryption. The Council stressed the need for cooperation between government agencies, particularly when dealing with crimes which take place across national borders (Council of Europe 1995).

In addition to these procedural guidelines, the Council of Europe has proposed that member states should enact uniform computer-related fraud and forgery legislation in the following terms (Council of Europe 1990):

> The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing that influences the result of data processing, thereby

> causing economic or possessory loss of property of another person with the intent of procuring an unlawful economic gain for himself or for another person.
>
> The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing in a manner or under such conditions which would, according to national law, constitute an offence of forgery if it had been committed with respect to a traditional object of such an offence.

Another initiative designed to produce consistent laws relating to electronic commerce is the Model Law on Electronic Commerce produced by the United Nations Commission on International Trade Law (UNCITRAL) in 1996. The Model Law sets out recommended legal provisions to remove any legal obstacles to the development of electronic commerce. As with the Australian legislation which has been proposed, and which was based on the Model Law, the Model Law itself was primarily designed to deal with civil issues relating to the law of contracts and evidence although its provisions which govern the recognition of electronic signatures and the admissibility of computer evidence have application to criminal prosecutions as well as civil proceedings. The Model Law has been adopted in full or in part in a variety of jurisdictions in the United States as well as in various European countries.

Arguably what is needed in order to ensure that criminal prosecutions may be taken in respect of electronic fraud against governments, is for existing criminal offence provisions to be amended to ensure that criminal laws accommodate the precise electronic transaction systems which will operate. Although many of the technical legal problems have already been solved through the amendment of various criminal and evidentiary laws, a number of problems remain.

Preventive and Control Strategies

A wide range of strategies have been developed to prevent government fraud which range from the creation of guidelines and policies on fraud control to the use of computer-based security techniques. These are presented in groups which range from those which arguably entail the least expenditure and which are likely to yield the greatest benefits, to those which are more expensive but less likely to be effective. Once again, this

arrangement is largely subjective and made in the absence of the results of any quantiative research into costs and benefits.

Management of Fraud Control

Most government agencies throughout Australia now have in place detailed fraud control policies which provide guidelines on ways in which to reduce the risk of fraud. The Commonwealth government, for example, has a comprehensive Fraud Control Policy which is currently being reviewed to take into account recent and emerging issues and risks.

Of particular importance is the need to develop specific policies on computer security with appropriate guidelines on reporting computer misuse and abuse. Australia now has public interest disclosure legislation which aims to ensure that those who report illegal conduct are not disadvantaged by their conduct. In the case of computer-based illegality, as in other areas of crime, severe penalties should be imposed on individuals who engage in, or attempt or conspire with others to carry out acts of reprisal against those who disclose illegality in the public interest. To date such remedies have rarely been used.

Policies also need to deal with specific on-line behaviour of employees. Agencies should establish guidelines, for example, on access to and use of the Internet for private purposes, personal use of electronic mail, downloading government software, and the use of copyright material. Although complete prohibition of such conduct may be unnecessary, clear policies need to be in place and explained to staff.

Personnel Monitoring

One of the most important areas in which technology-based fraud against governments can be contained lies in ensuring that trustworthy and reliable staff are employed, particularly in senior positions of responsibility. 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 within agencies 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.

Computer Usage Monitoring

Employees' use of computers and their on-line activities should 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. The filtering software 'Surfwatch', for example, can be customised to permit certain employees to be denied access to certain 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 the financial activities of government agencies also provides an effective means of detecting fraud and deterring individuals from acting illegally. The HIC, for example, employs artificial neural networks to detect inappropriate claims made by health care providers and members of the public in respect of various government-funded health services and benefits. The Commonwealth government also makes use of a complex database in its Parallel Data-matching Program to prevent taxation and social security fraud. The Program permits anomalies in payments to be identified and targeted for further investigation, and also enables individuals to be identified who are entitled to receive benefits which they have not claimed. In the year 1996-97, the Program resulted in direct net savings of A$132 million for two departments, Social Security and Employment, Education, Training and Youth Affairs (Centrelink 1997).

Personal Identification

Authentication of one's identity is crucial in preventing computer-based fraud in both the public and private sectors. At present, most authentication procedures involve the use of passwords or PINs. Ensuring that these are used carefully and are not able to be compromised

represents a fundamental fraud control measure. In addition to user education, a variety of innovative ideas have been developed to protect passwords and to enhance user authentication (see Alexander 1995). Systems are available which change passwords regularly, or which deny access after a specified number of consecutive tries using invalid passwords. Terminals have been devised with automatic shutdown facilities whilst challenge-response protocols and call-back systems have also been devised to check on the identity of users. Finally, space geodetic methods have been devised to authenticate the physical locations of users (Denning 1999).

In the future, many user authentication systems will make use of so-called biometric identifiers which make use of an individual's unique physical characteristics. Common examples include fingerprints, voice patterns, typing patterns, retinal images, facial or hand geometry, and even the identification of a person's subcutaneous vein structures or body odours (Denning 1999). Although such systems achieve much higher levels of security than those which rely upon passwords, they are expensive to introduce and raise potential problems in terms of privacy and confidentiality of the personal data stored on government computer networks.

The prevention of false identity fraud will become increasingly important when agencies begin using electronic commerce. Project Gatekeeper, for example, requires that individuals provide multiple and independent primary sources of identification when registering with public key Certification Authorities. At present, it is possible to submit documents which have been forged through the use of computerised desk top publishing equipment when opening bank accounts. This may also take place when individuals seek to obtain encryption key pairs from Certification Authorities. Steps would be required, therefore, in order to validate documents used to establish one's identity as well as to prevent the forgery of primary and secondary identification documents themselves.

Deterrence

The deterrent effects of criminal prosecution and punishment represent the final means of preventing fraud against governments. In addition to conventional judicial punishments such as fines and imprisonment, deterrence can also be achieved through professional disciplinary sanctions, civil action, injunctive orders and confiscation of an offender's

assets. Adverse publicity within government departments, such as publicised lists of Internet sites visited by staff, and forms of reintegrative shaming, could also be effective in workplaces where reputations are important.

Deterrent effects may also be achieved through the use of technology itself. One strategy developed to prevent software piracy, for example, entails the use of so-called Logic Bombs which are installed into programs. When activated through an act of unauthorised copying, the malicious code destroys the copied data and is even able to damage other software or hardware being used by the offender. Government employees who cause such damage would, presumably be personally liable for replacement costs and any consequential loss.

Conclusions

Computer technologies will greatly enhance the ability of people to defraud governments in the twenty-first century and already a range of instances of such conduct have begun to emerge. Many security risks simply replicate traditional forms of public sector illegality, but make use of computers to enhance the speed and efficiency with which they are carried out. Others, are directed at computer systems themselves either through theft of hardware and software or by using computers to transfer funds illegally.

A wide range of strategies exist to prevent and to control such crime, some of which make use of well-established fraud control practices, such as risk assessment and the provision of information to those most at risk, whilst others make use of the most recent digital technologies to prevent systems from being put to improper purposes or to detect illegal conduct immediately it takes place.

In ensuring that governments are not able to be defrauded in the twenty-first century, it will be essential for all those involved to work cooperatively in making use of the latest technologies of computer crime control. Although the public sector may be 'shrinking' in terms of the scope of its role in the delivery of services, there remain abundant opportunities for those with the necessary expertise and lack of scruples to compromise security procedures which have been put in place. Most likely, governments will need to call on the private sector to assist in devising effective means of combating fraud in the years to come.

Acknowledgments

An earlier version of this paper was published in the Australian Institute of Criminology's series *Trends and Issues in Crime and Criminal Justice*, No. 109, in April 1999.

References

Alexander, M. 1995, *The Underground Guide to Computer Security*, Addison-Wesley Longman Inc., New York.

Audit Commission 1994, *Opportunity Makes a Thief: An Analysis of Computer Abuse*, HMSO, London.

Australia, Model Criminal Code Officers Committee 1995, *Model Criminal Code Chapter 3: Theft, Fraud, Bribery and Related Offences*, Final Report, Australian Government Publishing Service, Canberra.

Australian Federal Police 1996-97, *Annual Report 1995-96, 1996-97*, Australian Government Publishing Service, Canberra.

Australian National Audit Office 1994, *The Australian Government Credit Card: Some Aspects of its Use*, Audit Report No. 1, 1993-94, Project Audit, Australian Government Publishing Service, Canberra.

Baer, P. 1996, 'The Australian Federal Police and Commonwealth Department Security Management', *Platypus Magazine (Australian Federal Police)*, No. 50, March, pp. 22-6.

Brandt, A. 1975, 'Embezzler's Guide to the Computer', *Harvard Business Review*, vol. 53, pp. 79-89.

Bridges, M. J. and Green, P. 1998, 'Tax Evasion and the Internet', *Journal of Money Laundering Control*, vol. 2, no. 2, pp. 105-14.

Campbell, R. 1999, 'DOFA Review in Wake of Alleged $8m Fraud', *Canberra Times* 17 February, pp. 1-2.

Centrelink 1997, *Data-Matching Program: Report on Progress 1996-97*, Data-Matching Agency, Canberra.

Council of Europe 1990, *Computer-Related Crime*, Recommendation No. R (89) 9, Council of Europe Publishing and Documentation Service, Strasbourg.

Council of Europe 1995, *Problems of Criminal Procedural Law Connected with Information Technology*, Recommendation No. R (95) 13, Council of Europe Publishing, Strasbourg.

Denning, D. E. 1999, *Information Warfare and Security*, ACM Press, Reading, Massachusetts.

Grabosky, P. N. and Smith, R. G. 1998, *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*, Federation Press, Sydney.

Health Insurance Commission 1997, *Annual Report 1996-97*, Australian Government Publishing Service, Canberra.

Health Insurance Commission 1998, *Annual Report 1997-98*, Australian Government Publishing Service, Canberra.

Hughes, G. 1998, 'Tax Staff Probed for Fraud', *The Age* (Melbourne), 16 September, p. 1f.

James, M. 1995, "Preventing the Counterfeiting of Australian Currency", in Grabosky, P. and James, M. (eds.), *The Promise of Crime Prevention: Leading Crime Prevention Programs*, Australian Institute of Criminology, Canberra, pp. 12-13.

Joyce, A. 1999, 'Cautionary Tales of Commonwealth Credit Card Fraud', *Comfraud Bulletin*, No. 12, January, pp. 2, 4.

KPMG 1999, *1999 Fraud Survey*, KPMG, Sydney.

Office of Government Information Technology 1998, *Gatekeeper: A Strategy for Public Key Technology Use in the Government*, Australian Government Publishing Service, Canberra.

Office of Strategic Crime Assessments and Victoria Police 1997, *Computer Crime and Security Survey*, Attorney-General's Department, Canberra.

Rastan, C. 1996, 'Not So Funny Money: Curbing the Counterfeiters', *Crime Prevention News*, March, pp. 17-19.

Tendler, S. and Nuttall, N. 1996, 'Hackers Leave Red-Faced Yard with $1.29m Bill', *Australian*, 6 August, p. 37a.