AUSTRALIAN INSTITUTE
OF CRIMINOLOGY

trends
&
issues

in crime and criminal justice

No.111

Defrauding Governments in the Twenty-first Century

Russell G. Smith

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 can 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, are described.

Adam Graycar
Director

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 taking an extended lunch break, to the serious, such as large-scale revenue fraud. In KPMG's most recent fraud survey, some 48 per cent of the 43 government organisations surveyed had experienced fraud in the preceding two years (KPMG 1997, p. 9).

Some of the largest losses sustained by governments result from the evasion of payments due to them (such as taxes and fees) and from 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 purposes. 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 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 online facilities. In the United Kingdom, for example, the government expects 25 per cent of all its 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).

April 1999

ISSN 0817-8542
ISBN 0 642 24100 7

Australian Institute
of Criminology
GPO Box 2944
Canberra ACT 2601
Australia

Tel: 02 6260 9200
Fax: 02 6260 9201

For subscription information together with a complete list of the papers in the Trends and Issues in Crime and Criminal Justice series, visit the AIC web site at:

http://www.aic.gov.au

or call AusInfo toll free on 13 24 47

The Commonwealth Government has developed a strategy, Project Gatekeeper, to provide a system of secure electronic communications when dealing with the government on public networks. It utilises public key cryptography and digital signatures (OGIT 1998). In Victoria, an online government service, *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://www.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, p. 30), 36 per cent of the 11 government agencies surveyed reported misuse of their computer systems, with 45 per cent reporting external forms of attack, that is remote access to computer systems. The computer abuse reported most frequently by the government agencies surveyed related to damage or unauthorised access to, or copying of, data and programs.

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 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 online 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 online transactions (see Bridges & Green 1998).

Customs and Excise. One area of particular concern relates to loss of customs and excise revenue through the illegal importation of electronic goods. The proliferation of digital copying systems has meant that it is now much easier than in the past to bypass customs controls by bringing digital goods, such as software, into Australia electronically, often via the Internet. In the future, customs controls on the movement of currency may also be circumvented where digital cash is brought into, or taken from, the country electronically.

Social Security and Health Benefits Fraud. As government benefits programs continue to be administered electronically, the opportunities for electronic fraud are enhanced. One recent case involved Centrelink employees who allegedly credited themselves with Electronic Benefit Transfer Cards, using both legitimate and false identities, to obtain illegal cash payments from the government (AFP 1998b).

Misappropriation of funds from the Health Insurance Commission (HIC) is also an area of considerable risk because of the large sums of money processed electronically through online claiming and payment systems. Between 1 July 1997 and 30 June 1998, 128,023 Medicare services (worth $7,461,353) were processed by electronic funds transfer. This was a relatively small proportion of the 202.2 million Medicare services billed in the same year, but will increase considerably in the future.

At present, the most common offences investigated by the HIC relate to claims for Medicare or Pharmaceutical benefits made using false or misleading statements. In 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, 2812 complaints of alleged fraud and inappropriate practice were recorded on the HIC's National Complaints Register (HIC 1998, Professional Review Supplement, pp. 17–18).

The HIC has already been subject to fraud perpetrated by insiders and it is possibe that those with the technological skills could attack its 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 1997, 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 that could be stolen prior to use. A survey by the Department of Finance and Administration found that, in the year to April 1998, there were 11,287 Australian Government Credit Cards which were used for 484,000 transactions with a total value of $162 million (Joyce 1999).

Transacting government business through the use of credit cards raises all of the security risks which cards bring with them (see Grabosky & Smith 1998, ch. 8). More important, 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 46 cases of fraud reported for all departments and agencies, totalling $1.8–2 million. The bulk of cases were for claims under $5000, 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. The Civil Aviation Safety Authority, for example, recently identified two cases in which its officers had abused Travelcards issued for official business. One had withdrawn his travel allowance from the authority’s bank, then used his Travelcard to pay for accommodation, meals, drinks and in-house videos whilst on official business. Another used his Travelcard as a form of personal credit line, withdrawing cash and repaying it later, when convenient (Joyce 1999).

Theft of Telecommunications Services. Government operations rely to a great extent on the use of telephones and fraud 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 use digital technologies to compromise the security features of cellular telephones. Previously, carriers were wholly owned by governments, but 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, hackers based in the United States gained illegal access by computer to Scotland Yard’s PABX system in London. 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, p. 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 be victimised through acts of forgery and counterfeiting carried out using desktop publishing equipment (personal computers, scanners and colour printers) (Baer 1996). Counterfeiting of currency issued by central banks has been greatly facilitated by these technologies, which have also been used to forge government cheques, benefit claim forms and payment vouchers, and 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. Another case in Perth allegedly involved a 23-year-old university student who had used computer systems to counterfeit $100 notes (AFP 1998b).

Theft of information

The Australian Federal Police have also investigated cases in which employees gained unauthorised access to Commonwealth computers, copied data illegally and sold copies to third parties (Baer 1996, p. 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 (AFP 1996, p. 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 after he was found guilty of unlawfully gaining access to, and disclosing, departmental information (AFP 1997, p. 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, but the greatest risk 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 greater. In one case in 1997, a high-ranking CIA agent in the United States attempted to locate sensitive information within the agency's computerised databases. 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, p. 133).

Theft of computer hardware and software

Government employees are also in a position to steal computer equipment that often contains valuable software and sometimes sensitive information. In a recent investigation 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 has since undertaken a review of its security and employee screening procedures to prevent similar incidents occurring (AFP 1998a, p. 43).

Theft of time

Finally, one of the most difficult-to-detect types of computerised theft is the theft of time (and incidentally, electricity). This occurs when employees make unauthorised personal use of computers 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 to government operations.

Large-scale misuse of government resources in this way results in lost productivity, creates an inappropriate culture in the workplace and could, potentially, lead to problems of legal liability. The area of greatest 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 20 people had each visited more than 1000 sexually explicit sites in less than a month. In a survey of executives conducted by *PC World*, 20 per cent of the 200 companies surveyed had disciplined staff for misusing Internet access, the most common offences involving visits to pornographic web sites, shopping, using chat lines, gambling and downloading illegal software (Denning 1999, pp. 360–1). Although an equivalent survey of government employees' use of the Internet has not been conducted, it is likely that similar behaviour would be present.

In order to combat such problems, many government agencies monitor the activities of their employees, sometimes covertly through video surveillance or by 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.

Preventive and Control Strategies

A wide range of strategies have been developed to prevent government fraud, ranging 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 but are likely to yield the greatest benefits, to those which are more expensive but less likely to be effective. Again, this arrangement is largely subjective and made in the absence of the results of any quantitative research into costs and benefits.

Management of fraud control

Most government agencies throughout Australia now have detailed fraud control policies in place to provide guidelines on ways 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 to ensure that those who report illegal conduct are not disadvantaged by their action. 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.

Policies must also deal with specific online 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 should 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 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 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 effective risk management procedures within agencies, 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, and the influence to carry it out.

Computer usage monitoring

Employees' use of computers and their online activities should be monitored using logs so that managers know whether staff have been using the Internet for non-work-related activities. The filtering software "Surfwatch", for example, can be customised to deny certain employees access to certain content. 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 employs artificial neural networks to detect inappropriate claims made by healthcare 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 identifies anomalies in payments, targets these for further investigation and also identifies individuals entitled to receive benefits they have not claimed. In 1996–97, use of the program resulted in A$132 million direct net savings for two departments: Social Security and Employment, Education, Training and Youth Affairs (Centrelink 1997).

Personal identification

Authentication of an individual'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 cannot 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 utilise 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 forged on desktop 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, 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 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. Others make use of the most recent digital technologies to prevent systems from being used for improper purposes or to detect illegal conduct immediately it takes place.

In ensuring that governments cannot 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 already 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.

References

Alexander, M. 1995, *The Underground Guide to Computer Security*, Addison-Wesley Longman Inc., New York. Extracts at http://www.securitymanagement.com/library/000273.htm

Australian Federal Police (AFP) 1996, *Annual Report 1995-96*, AGPS, Canberra.

Australian Federal Police (AFP) 1997, *Annual Report 1996-97*, AGPS, Canberra.

Australian Federal Police (AFP) 1998a, *Annual Report 1997-98*, AGPS, Canberra.

Australian Federal Police (AFP) 1998b, *Newsletter of the Australian Federal Police*, December.

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

Baer, P. 1996, "The Australian Federal Police and Commonwealth department security management", *Platypus Magazine: The Journal of the 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. & 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.

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

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

Health Insurance Commission (HIC) 1997, *Annual Report 1996-97*, AGPS, Canberra.

Health Insurance Commission (HIC) 1998, *Annual Report 1997-98*, AGPS, Canberra.

James, M. 1995, "Preventing the counterfeiting of Australian currency", in *The Promise of Crime Prevention: Leading Crime Prevention Programs*, eds P. Grabosky & M. James, 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 1997, *1997 Fraud Survey*, KPMG, Sydney.

Office of Government Information Technology (OGIT) 1998, *Gatekeeper: A Strategy for Public Key Technology Use in the Government*, AGPS, 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. & Nuttall, N. 1996, "Hackers leave red-faced Yard with $1.29m bill", *Australian*, 6 August, p. 37a.

Dr Russell G. Smith is a Research Analyst with the Australian Institute of Criminology.

General Editor, Trends and Issues in Crime and Criminal Justice series:
Dr Adam Graycar, Director
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601 Australia

Note: Trends and Issues in Crime and Criminal Justice are refereed papers.