

Crime at work

- [1. Introduction](#)
- [2. Crime against business: the big picture](#)
- [3. Crime by business](#)
- [4. Violence, bullying and harassment](#)
- [5. Fraud and deception](#)
- [6. Fraud against government](#)
- [Wind-up](#)
- [Additional Resources](#)

1. Introduction

In February 2003, there were 9,516,000 Australians in employment. A large number of Australians also work as volunteers—an estimated 4.4 million Australians (29 per cent of people aged 15 years and over) undertook voluntary work through a group or organisation during 2000.¹ Many of us spend more waking hours at work than anywhere else. What happens at work can have a big influence on us and on the people around us.

A range of crimes happens in the workplace. Some crimes, such as shoplifting, are committed against business by customers, staff or others. Some crimes are committed by business, like tax evasion, fraud or illegal dumping of waste. Sometimes outside disputes spill over into the workplace. Some crime happens between staff, like theft, assault or on-line stalking.

Sometimes individuals are the victims. Sometimes an organisation or business is the target. But in most cases, crime at work affects not just the victim but other workers, the whole organisation and often the broader community as well if it increases business costs.

Crime against business touches the lives of many people. The community helps to pay for the significant costs to business resulting from crime through higher prices, charges or insurance premiums. If crime reduces profits there will be less money to share with staff or shareholders.

This module looks at crime against business, crime by business and crime in the workplace generally. It touches on the costs to business and the community, and what might be done to prevent crime and manage the risk of crime. It explores a number of specific crimes, including workplace violence and bullying, fraud, tax evasion and environmental harm.

2. Crime against business: the big picture

Businesses and organisations are the victims of a range of crimes, including burglary, shoplifting, theft by employees, customers or suppliers, vandalism and graffiti, arson, robbery, assaults against staff, abusive and threatening behaviour towards staff, damage of and theft from company vehicles, and fraud. Despite this, crime against business doesn't get widely reported.

In spite of evidence that crime against businesses is a considerable proportion of all crimes ... these crimes generally escape the attention of the traditional surveys of crime. Police and other data indicate that, pro rata, businesses are considerably more at risk of certain types of crime than are households, and that the costs of crimes against businesses are a significant imposition on business.

John Walker, 'Crimes against businesses in Australia', Australian Institute of Criminology, Trends and issues in crimes and criminal justice No. 45 (p.1).

It's difficult to identify the total losses to business from crimes like robbery, theft (both physical and electronic) and burglary, but they are probably greater than published estimates. While businesses are increasingly willing to share such information among themselves, there is some fear that publicising losses could either encourage crime (if they are seen as an easy target) or damage workplace morale (where employees are responsible for the crime).

In some cases, the loss from a single crime may be small, but because it happens often, the total cost is high. For example, one milk company estimates it loses more than \$3.5 million a year as a result of theft and misuse of its plastic milk crates.² Theft and misuse of shopping trolleys cost many millions of dollars when you add up replacement costs and fines paid to local councils to recover abandoned trolleys. Some centres have introduced expensive measures to protect shopping trolleys such as coin-in-the-slot mechanisms.

Discussion starter

- Have you seen examples of robbery, theft, fraud or shoplifting in the workplace? If you feel comfortable, you might talk about the circumstances and your response. Do you know what motivated the crime?
- Has anyone in the group had to deal directly with a crime against a business (or know someone who has)? In your experience, how much time was spent dealing with police, insurance companies, customers and suppliers? What was the effect on the business? What had the most impact—the crime or its flow-on effects?

Computers and corporate vulnerability

The widespread use of computers in business has opened up a new source of vulnerability: we are now vulnerable to sabotage, theft (via the electronic transfer of funds and phishing), blackmail and extortion, and piracy. [Phishing' is described below] Computers have multiplied the potential impact of data manipulation and financial fraud. They have made it easier to disguise the proceeds of crime through multiple electronic transfers of funds. While there is a growing business developing security measures to protect data, ways of overcoming these are often only a few paces behind.

Information technology has also created new categories of crime, such as computer hacking, theft of electronic information and the creation of computer viruses. In 1999, an Australian Federal Police investigation led to a conviction and what is believed to be the first gaol sentence in Australia for computer hacking. A man who broke into the computer system of Internet Service Provider AUSNet, causing actual and potential commercial harm, was sentenced to three years gaol, with a non-parole period of 18 months (R v Stevens [1999] NSWCCA 69 (15 April 1999)).

Discussion starter

- Has anyone in the group experienced computer-related crime at work? What was the story? What was the impact?
- Deliberate, hostile employee misconduct, such as sabotage of information or damage to the reputation of the business, is usually closely linked with low workplace morale. Do you think companies take the issue of employee morale seriously enough?

An increase in attacks by electronic viruses and other computer crime has been significant on Australian businesses and the public sector in recent times.

The survey of over 17 private industry sectors and all tiers of government found that the average annual losses for electronic attack, computer crime or computer access misuse or abuse had increased to \$116,212 per organisation compared to 2003.

AusCERT, Australia's national computer emergency response team, based at the University of Queensland, Brisbane, produced the survey in conjunction with Australia's law enforcement agencies.

The survey results provide valuable information to help police across Australia fight computer crime.

Other key findings of the survey were:

- More organisations experienced electronic attacks that harmed the confidentiality, integrity or availability of network data or systems (49 per cent in 2004 compared with 42 per cent in 2003).
- Most of the attacks were sourced externally (88 per cent) compared to internally (36 per cent), but fewer organisations experienced external attacks compared with 2003 (91 per cent);
- For the third consecutive year, infections from viruses, worms or trojans were the most common form of electronic attacks reported. They were the greatest cause of financial losses, accounting for 45 per cent of the total losses for 2004, followed by laptop theft and abuse and misuse of computer network access or resources.
- On average, losses reported by Critical National Information Infrastructure (CNII) organisations (\$98,685) were almost double average losses for non-CNII organisations (\$56,531).
- While respondents to the survey said they had taken steps to improve their IT systems, fewer reported that they were managing all computer security issues reasonably well (5 per cent this year compared with 11 per cent for both 2002 and 2003).
- The survey reported that efforts by organisations to protect their IT systems did not appear to be keeping pace with the changing nature of threats and vulnerabilities, particularly the increased number and severity of system vulnerabilities and the number and rapid propagation of Internet worms and viruses.

Other security management findings were:

- The most common difficulties for organisations were changing user attitudes and behaviour (reported by 65 per cent of respondents), and keeping up to date with information about the latest computer threats and vulnerabilities (61 per cent).
- Unpatched or unprotected software vulnerabilities (reported by 60 per cent of respondents) and inadequate staff training and education in security practices (49 per cent) were the two most common factors contributing to harmful electronic attacks.
- The need for greater understanding or support for IT security issues from senior management was important to 45 per cent of respondents.

The survey shows that infection from viruses, worms and trojans is currently the most serious issue facing businesses—both in terms of the high number reporting financial loss and the high cost of these attacks. One disturbing aspect of this trend is the use of malicious codes to surreptitiously steal e-commerce authentication information such as on-line banking passwords. AusCERT has seen the development and evolution of new trojans designed specifically to target e-commerce users for illicit financial gain.

The increase in computer or electronic crime (e-crime) has been reported by a number of businesses and includes a scam called *phishing* which is a form of unsolicited commercial e-mail designed to access and manipulate financial accounts. The e-mail usually asks for details of accounts such as account numbers and passwords purportedly to correct or update customers' details. The difficulty

for the majority of people in detecting the scam is that the fraudsters use clever techniques to make the websites including those of banks, look authentic. E-Bay and PayPal have been vulnerable to phishing as have some major banks, including Westpac.

Both business and private computers are also vulnerable to trojans. Again, cleverly devised, trojans appear to be legitimate programs but contain a function, such as a password feature which enables fraudsters to hack into and take over the computer. Sometimes these programs contain viruses which anti-virus scanners may not detect.

Other crimes to watch out for include *identity theft* and *data diddling*:

Identity theft is when a criminal takes your personal information, like name, tax file number, etc and uses it to establish credit and charge items to you. Identification cards and credit cards are applied for using your personal information and once the credit cards are issued, the bills start rolling in.

Data diddling involves modification of data while it is being keyed or processed into the computer. It can include cancelling debts without proper authority or reducing outstanding amounts of monies owed.

Salami slicing is similar to data diddling; however, it refers to predominantly financial transactions. It is where a slight fraction of money is “sliced” or taken off the principal amount and accumulated. For example, wage payments could be rounded down and the fractions are accumulated and credited to the perpetrator’s own account.

(This information is provided by the Entrepreneur Business Centre. For small business products and services, visit www.abc.com.au).

If you’re interested in finding out more about computer-related crime, you might contact the School of Business Information Technology Centre at the Royal Melbourne Institute of Technology (RMIT), Ph (03) 9925 5969, fax (03) 9660 5850 or try their website at:

<http://www.rmit.edu.au/bus/bit/> Other sites include Internet Industry Association, Security Portal <http://www.security.iaa.net.au/> AusCERT <http://www.auscert.org.au/>

\$32 billion, the high cost of crime.

Crime and the cost of fighting and dealing with it costs Australia about \$32 billion annually, according to the Australian Institute of Criminology.

In a report to be released today, the institute includes costs such as medical treatment and lost productivity from victims of assaults and homicides, property lost in burglaries and car thefts, credit card and employee fraud, and arson and vandalism.

Institute director Adam Graycar said the report revealed the hidden costs of crime. Estimating its costs was important in directing law enforcement into areas where it would be of most benefit, he said.

Among the findings:

- Each homicide costs \$1.6 million, mostly in lost productivity from victims. The total cost of homicides was \$930 million in 2001, the survey year.
- Lost productivity and health costs related to drug abuse and drug treatment programs cost \$1.96 billion.
- Violent and property crime attributed to drug dependency costs an estimated \$3.7

billion, putting the total cost of illicit drugs at \$5.6 billion.

- Residential burglaries cost about \$1.7 billion, and burglaries overall cost \$2.43 billion.
- Fraud, comprising credit card abuse, welfare, tax, insurance fraud and forgery costs the public \$5.8 billion a year.

Many of the figures are estimates. The report attempts to take account of unreported crime, using measuring methods used overseas.

The most careful costings are those for homicide, assault, sexual assault, robbery, burglary, car theft and shoplifting, the report says. But calculating the cost of fraud is ‘particularly tenuous’. Dr Graycar said most frauds were not investigated by police, and businesses were reluctant to report it for fear of being seen as naive and an easy mark.

The report estimates that three frauds go undetected for every one recorded.

The costs attributed to drug offences do not include policing and prosecuting offenders, and the cost of homicides does not include investigations or imprisonment of offenders, which costs about \$50,000 each a year.

Police Minister Andre Haermeyer said he had ‘some difficulty with being too driven by putting values on things that are too difficult to evaluate. How do you put a value on homicide? Certainly it (the report) tells us crime has considerable costs.’

Victoria Police Association secretary Paul Mullett said the report highlighted that proper resourcing of police saved money in the long term.

He called on the state government to provide the 600 extra police it had promised so that more resources could be directed to crime prevention.

The Age, 9 April 2003.

The cost of crime in Australia

Criminal justice system	\$6.4 billion
Private security industry	\$3.1 billion
Fraud	\$5.8 billion
Crime and health costs of drug abuse	\$5.6 billion
Homicide	\$930 million
Car theft	\$880 million

Australian Institute of Criminology. 2003.

A 1999 survey of crime against small business conducted by the Australian Institute of Criminology looked at five sectors of industry, including retail food, retail liquor, newsagencies, pharmacies and service stations. Of the Australia-wide sample, 51.1 per cent experienced crime in the period of the study. The most common crimes were theft from premises, followed by burglary, vandalism, credit card fraud and employee theft. Many small businesses experienced repeat victimisation—mostly for credit card fraud, vandalism, assault/threat/intimidation, employee theft and burglary. The study found that businesses were most vulnerable in their first four years of operation and medium-sized businesses were victimised more than very small businesses.³

A 1997 survey of the South Australian retail sector found two-thirds of those surveyed had experienced crime against their business or customers in the previous year. Crimes included theft of stock, break and enter, arson, robbery, vandalism, unexplained stock loss ('shrinkage'), and theft by staff. The survey found that the vast bulk of crime against retailers occurs without their even realising a crime has been committed. Stock shrinkage as a result of theft by customers and/or staff accounts for almost 70 per cent of the state-wide figures.

Discussion starter

- Is anyone in the group involved in business? Is crime a problem for that business? What steps have been taken to prevent crime?
- Some people believe that taking home the occasional pad or pen or folder for non-work purposes is fair compensation for the extra time they work without being paid. In some workplaces, long lunches or an afternoon off are accepted as a way of making up for extra hours worked when things are busy. Should the two things be treated the same way? Why/why not? What about someone who regularly takes long lunches or arrives late to work and affects the productivity of other workers and business profits? Is this theft of profit? Should it be treated as a crime?

Shoplifting

Shoplifting or theft of stock is one of the main crimes faced by retail businesses.

Who's doing it?

It wasn't a crime of need, and she doesn't think of herself as a thief—she is one of the 'opportunistic' shoplifters the store security experts say lurk within most of us. Remove the perceived threat of being caught ... and up to 80 per cent of Australian shoppers would seriously consider snatching something up for free.

Stores are faced with what they say is an increasing wave of shoplifting, caused largely by the heroin explosion, the boom in gambling and the arrival of highly organised shop-stealing rings so brazen as to run decoy shoplifters while they steal to meet their clients' 'orders'.

... the problem [is] costing Australian shops about \$2.7 billion a year (or 2–4 per cent of the \$135 billion turnover), and one the industry regards as so sensitive it observes a virtual code of silence on the subject ...

The difficulty for industry is that ... no two shoplifters behave the same way, take the same things, or have the same reasons for doing it. Also, half the retail theft in Australia is perpetrated by employees, who can be virtually impossible to catch.

Of the external thieves, security experts categorise them as: professional thieves (who sell the goods from their own black-market 'shops'); semi-professionals—people who love to shop, and who can manipulate the system, find the weakness in the store; teenagers after a thrill; drug addicts; kleptomaniacs (stealing addicts); and by far the biggest group, opportunistic or impulsive thieves.

Wendy Tuohy, 'Thieves like us', The Sunday Age, 25 April 1999.

In 2002–2003, Victorian police found that 54 per cent of those caught shoplifting were male and 46 per cent female. Boys (57 per cent) outnumber girls (43 per cent) in the 15–19 age group. But

women were 62 per cent of those aged 25–34 and 61 per cent of those aged 36–45. Older Australians aged over 65 made up 22.4 per cent of all shoplifters identified in this survey, with men outnumbering women. When caught, many said their pensions were inadequate. Boredom and mental illness were also factors.¹

Shoplifting by age group

10–14	14.1 per cent
15–19	22.9 per cent
20–24	14.2 per cent
25–34	23.0 per cent
35–44	12.8 per cent
45–54	5.9 per cent
55–64	3.5 per cent
65 and over	3.6 per cent

In high-tech, gizmo-rich Japan, mobile phones able to take digital photos have fast become mandatory accessories. They have also quickly become the latest tool for a new crime—digital shoplifting.

The crime is deceptively simple. In the crowded bookstores, the digital shoplifter is deftly able to record images from magazines to be viewed later.

Japan has a long tradition of allowing people to leaf through publications, a tolerance made easier because thumbed copies can be returned to the publishers.

But digital shoplifting has taken this to a new and costly level, to the point where publishers have decided to fight back.

Under a new campaign unveiled by the Japan Magazine Publishers Association, mobile phone users are being urged to ‘refrain from recording information with camera-mounted cell phones and other devices’.

Mobile phones capable of taking digital photos have also been used for crimes other than ‘shoplifting’ magazines. The media have reported cases of the phones being used to take photos up women’s skirts on crowded trains.

The potential for the problem to emerge in Australia was demonstrated recently, with moves to ban mobile phones from the changerooms of gyms, pools and sports centres.

The Sydney Morning Herald, 30 June 2003.

Shoplifters : Retail Feels The Pinch

Shoplifting, costing retailers as much as \$1.5 billion a year, is the most under-reported property theft, taking out as much as a quarter of the annual profit of a business..

And while cost-recovery programs were proving popular overseas as a means of reducing shoplifting’s impact, Australian retailers still had to take independent action if they wanted to be paid for some of the cost of policing their stores.

The Australian Retailers Association estimated shrinkage at 1.8 per cent of retail sales, equivalent to about \$2.5 billion a year. Employee and customer theft made up 35 per cent each and administrative errors and wastage 30 per cent.

While that would indicate that each form of theft cost \$875 million a year, Renata Ringin, managing director of Victorian-based loss-prevention service Pro Active Strategies, believed that figure could be higher.

Ms Ringin, who completed a study of retail civil recovery programs on a Churchill Fellowship, said shoplifting customer theft costs retailers as much as \$1.5 billion a year.

‘Shoplifting could be seen as the largest and fastest-growing property crime, with significant economic cost to the community,’ she said. It was also the most under-reported.

She estimated shoplifting now represented 55 per cent of property crime, compared with 32 per cent in 1995.

Among the reasons retailers gave for not reporting the crime was the belief that police could not do anything. Also, they did not consider it serious enough to report, which was associated with the view that chances of a successful conviction, other than a rap over the knuckles, were slight.

But shoplifting could do serious damage. ‘In terms of retail margins, the cost of shrinkage at 1.5 per cent of total sales can equate to a 25 per cent loss in profit and can make a business unviable,’ Ms Ringin said.

Australian Financial Review 30 September 2003.

Discussion starter

You might like to break into small groups for your discussion so everyone gets more of a say.

- Does any of the information in this Victorian survey surprise you? Why/why not?
- Half the retail theft in Australia is committed by employees. How would you try to reduce theft by employees?
- Do you agree that most people would be tempted to steal if they thought they wouldn’t get caught? Why/why not?
- Has anyone ever shoplifted (or known someone who has)? What was the motivation? What was taken? How could businesses reduce the amount of shoplifting? Would it be possible to limit the goods on display?
- If it is true that drug-taking and gambling are causing an increase in shoplifting, how do you think the problem should be tackled?

The ‘down side’ of a consumer culture?

Businesses and organisations spend billions of dollars each year to encourage us to buy their goods and services. A lot of advertising links the purchase of an item with being young or cool or successful or beautiful. Advertising is a key tool used by business to gain an advantage over their competitors. It is part of our contemporary market system.

At the same time, globalisation and increased competition has been accompanied by a growing divide between rich and poor in Australia—and many other countries as well. So at the very time that more is being spent than ever to convince us to buy goods and services, more people are finding it difficult to make ends meet.

Discussion starter

- Businesses sometimes use advertising and shop displays that suggest your life would be better if you had their product or service. Do you think that by doing this business encourages shoplifting?
- Is it possible to change how goods and services are marketed without hurting sales?

Ideas for reducing shoplifting

It's not often a surveillance salesman tells you that even the best security system could be a waste of money. But that's the message Direct Security manager of corporate services Brian Dureau wants business to hear.

While he advocates installing digital surveillance systems—especially from his company—Mr Dureau says a crucial but often neglected way to prevent shoplifting is staff training.

'It's all right to buy a surveillance system, but staff have to know what to look for to prevent shoplifting in the first place,' he said.

'From the business's point of view, it isn't about catching shoplifters and taking them to court, but actually stopping them targeting the business.'

But just as no security system is thief-proof, relying on good customer service alone to prevent shoplifting can be dangerous, as boutique retailer Husk found out the hard way.

The business has been operating since 1995 in one store in Toorak and one in Albert Park, specialising in local fashion, cosmetics and crafts.

General manager Susie Stanford says that for most of that time, the company assumed shoplifting wasn't an issue.

'As a boutique, we thought we'd be isolated from the problem, because the way we serve is quite intensive, as opposed to a larger store where it's all self-serve,' she said.

Late last year, they realised they had been wrong, and seven weeks ago had a security tag and surveillance system installed.

Ms Stanford says a typical retailer loses between 0.5 per cent and 1 per cent of turnover to shoplifting, but that Husk stores were losing around 2 per cent to 3 per cent before they invested in the extra security.

It still hasn't stopped shoplifting: staff know of three incidents in that time, including one involving a regular shopper, who may actually have been a regular shoplifter.

So this week the Husk staff will sit down with Mr Dureau and review the surveillance tapes, using the 'regular shopper' incident as a training exercise, to find out what they could be doing better.

'As well as acting as a deterrent during peak times, the system is also about making everyone face the cold hard facts of shoplifting,' Ms Stanford says. 'If we can see that we haven't done as well as we could have in protecting ourselves, then that's a real opportunity to train and improve.'

The retail manager at Husk's Albert Park store, Sally Bailey, has worked in retail since 1990, and agrees that a well-trained retail worker can spot most shoplifters in the crowd.

'Shoplifters can be anyone, but their actions tend to give them away.'

'They do a lot of touching of stock, as well as looking back around the store to see who's around. It can be really quite obvious when you know what to look for.'

Ms Bailey says, in her experience, good service is the most effective deterrent to shoplifters.

So far, no one has come up with a way to eradicate the problem, but retailers such as Husk hope at least to cut their losses.

Mr Dureau says the hardest part is finding the balance between security and good service: 'After all, you want people to feel happy when they walk into your shop, not like they're going to be body searched.'

The Age 3 April 2002

Discussion starter

- What approach should/could businesses take to reduce the incidence of shoplifting? Are you aware of shops in your area which appear to have developed a non-intrusive prevention process?
- Is there anything customers can do to help business address the problem of 'shrinkage'?
- If you want to explore this issue further, you might ask a representative from the local chamber of commerce or retail centre to talk to the group about the costs of shoplifting, its impact on business and the community, and ways that the group could help.

3. Crime by business

While most business is legitimate, some businesses are themselves involved in illegal activities, like importation of drugs or financial scams. Others use illegal practices to cut costs or save money—for example, illegal dumping of waste, or evading tax by paying staff in cash. Sometimes businesses commit offences because they fail to maintain plant and equipment properly or to supervise work or manufacturing processes.

Discussion starter

- What factors do you think might encourage a business to behave illegally?
- Do you think high levels of competition between businesses and organisations increase the risk of illegal behaviour?

Software piracy and computer counterfeiting

Illegal copying of computer software causes real losses for the writers (or licensors) of that software. Often the offenders are businesses that install more copies of software than their licence allows or individuals that make copies for colleagues and friends. At the High-Tech Crime Conference held in the United States in 1997, software piracy was claimed to cost US firms 35 per cent of their

business.¹

According to the Business Software Association of Australia (BSAA), research estimates that in 2003, 31 per cent of all PC software in use in Australia was illegal—an improvement from the 50 per cent estimated in 1989 when the BSAA was formed.² Penalties for companies and individuals are not insignificant; an offence is liable for a \$93,500 fine or up to five years imprisonment for an individual and a \$467,500 fine or up to five years imprisonment for a company.

Counterfeiting is also a significant problem. According to Microsoft's chief investigator, counterfeit Microsoft mice were costing the business 'US\$200,000 a month in losses plus hundreds of returns to consumers because the mice don't work properly'.³

Discussion starter

- Has anyone in the group ever been involved with (or known someone who is involved with) illegal use of software? If you feel comfortable, you might talk about the circumstances.
- Should software piracy and illegal copying of software be crimes?
- For heavy fines to be an effective deterrent, people need to believe they face a real risk of getting caught. In your experience, do people take illegal copying of software seriously? How do you think software theft could be reduced?

If you're interested in finding out more you could contact the Business Software Association of Australia hotline: 1800 021 143 or their website, <http://www.bsaa.com.au/>.

Environmental crime

Governments in Australia (and around the world) are recognising the importance of balancing economic development with the preservation and protection of the natural environment for future generations.

There are many laws, regulations, policies and guidelines in each state and territory to help protect the environment and to give guidance to business and industry. These laws and guidelines cover such issues as water and air pollution, waste management and the use and disposal of hazardous material. If you would like further information about the environmental laws in the different states and territories, see the Australian Government Department of the Environment and Heritage's website at <http://www.deh.gov.au/>.

Concern about the behaviour of polluters and increased public interest in environmental issues has led governments in Australia to increase criminal sanctions and widen criminal offences for harming the environment. Many breaches of the law involve serious penalties and in most instances the prosecutor need not prove that a person intended to cause the incident. Even accidents which cause environmental damage can result in prosecution.

- In Victoria, for example, in June 2002 the government increased the maximum fines for general pollution offences from \$20,000 to \$240,000 and increased the maximum fine for dumping industrial waste from \$40,000 to \$500,000.⁴
- In New South Wales, the most serious offences are for wilful or negligent breaches of the law that result in harm to the environment. These offences carry penalties of up to \$1 million dollars or seven years gaol. The maximum penalties for most pollution offences are \$250,000 for companies and \$120,000 for individuals.⁵
- At the Australian Government level, in 1999 the government introduced tougher penalties,

including gaol terms of up to 10 years for illegal dumping of waste at sea. The offence of dumping radioactive material now attracts a gaol term of up to 10 years and a fine of up to \$210,000 compared to about \$50,000 previously. Corporations convicted of these offences will be liable for up to five times these penalties.⁶

Case example: Corporate pollution

Charges have been laid against mining giant Energy Resources of Australia (ERA) after drinking water at its controversial Ranger Mine in the Northern Territory became contaminated with uranium.

Twenty-eight workers fell ill after the water supply at the site in Kakadu National Park became contaminated with uranium in March [2004].

An investigation by the Office of Supervising Scientist, Arthur Johnston, in August found the mine's radiation clearance measures and water systems were inadequate, with leaky pipes and broken valves common around the mill.

An NT government report in May recommended ERA be prosecuted over the incident.

Department of Business, Industry and Resource Development (DBIRD) chief executive Mike Burgess said charges were today filed in the Darwin Magistrates Court against ERA.

'The charges have been laid under sections s39 and s23(5) of the Mining Management Act,' Mr Burgess said.

'Section 39 carries a maximum penalty for a corporation of \$137,500 and section 23(5) a penalty of \$27,500.'

Mr Burgess said the incident was serious, and the findings of the departmental inspectors and those of the OSS showed that it was appropriate to bring the matter before the court.

The Courier Mail 29 September 2004

Discussion starter

- Given the importance of the environment to our quality of life, do you think we take environmental crime seriously enough?

Deterring environmental damage

Some commentators argue that criminal law is not a good way of preventing or minimising environmental harm for the following reasons:

- Environmental problems are not always immediately obvious and can continue well after the activity that caused the problem—for example, contaminated land or groundwater. By the time a criminal charge is brought, the damage is done.
- There will never be enough resources to catch the polluters who dump waste in the middle of the night.
- For big corporations, even fairly large fines may not be a real deterrent if it would cost them more to change how they operate in order to prevent the problem.

Criminal law, they argue, should be kept for persistent and severe breaches of the law, to punish rogue polluters. Regulation, education and cooperation between government, industry and the community should be the main tools for preventing environmental harm.

Others argue that criminal sanctions are important because they show that environmental harm is not socially acceptable. Over time, this will help change attitudes.⁷

Discussion starter

- Some commentators argue that criminal sanctions only punish misbehaviour—they do not demand change from corporations. Would it be possible to develop criminal penalties that do encourage change? For example, academics Brent Fisse and John Braithwaite⁸ argue that sanctions which affect values that are important to the corporation, such as profit, prestige and stability, are likely to be a greater deterrent than fines which become simply another business cost. Sanctions such as adverse publicity, community service or a compulsory re-direction of company shares to environmental interest groups could be considered. Alternatively, companies could be put ‘on probation’ or required to show that they have changed the way they operate. They could be ordered to work with local communities to develop an environmental improvement strategy that the community would monitor, in conjunction with the environmental protection agency.

Tax fraud

Tax is the way that our community funds a wide range of expenditure—defence and education, environmental protection and assistance to families, Medicare and road maintenance. Community willingness to contribute depends in part on people’s confidence that those who are required to pay tax under the law are paying it. Identifying and prosecuting fraud and tax evasion is important to ensuring that everyone pays their fair share, that rates of tax are no higher than they need to be and that the Government gets the revenue it needs to fund social expenditure.

Media reports of court cases brought against major corporations claiming unpaid tax are often accompanied by comment on talkback radio suggesting the big end of town gets away with things that ordinary people can’t. They claim that ordinary taxpayers are paying more than they should because companies that can afford fancy advice are not paying what they should. Reflecting similar public concerns, one of the Government’s arguments for the GST is that it will ensure that businesses dealing in cash to evade tax will have to pay some tax.

Tax evasion

Twenty-four of Australia’s 600 richest people repaid the tax man almost \$1 billion last financial year.

By tightening auditing procedures on big business and wealthy individuals, the Australian Taxation Office collected an additional \$4 billion last year.

Of that, \$918.7 million was extracted from the bank accounts of 24 of the nation’s richest by the ATO’s 100-member High Wealth Individuals Taskforce.

The office defines a wealthy individual as someone who controls or owns net wealth of more than \$30 million. An ATO spokesman confirmed about 600 people were currently

identified in that bracket.

However, about \$910 million of the \$918.7 collected is in dispute and the disputes are destined for the courts. But rich tax defaulters can expect to pay breach notices totalling \$451.5 million.

‘These results demonstrate our determination to responsibly pursue the more difficult and complex issues at the top end of the market,’ [then] Commissioner of Taxation Michael Carmody said yesterday.

The total tax collection for 2001–02 was \$168.6 billion, which included a net increase of \$363 million in GST collected from the previous year, as GST awareness programs became more widespread.

Mr Carmody said the black economy also came under greater scrutiny, with 2200 tax office staff sent into the workplace to eradicate under-the-counter payments.

Promoters of illegal tax schemes were also targeted, and nine such schemes were referred to the federal police for investigation. Tax evasion was also rife, with 117 people convicted and 59 of those receiving jail sentences. Another 400 such cases were under investigation or before the courts.

The Australian 1 November 2002

Discussion starter

- Have you seen examples of tax fraud? In your experience, is it a significant problem? Would you consider paying the cleaner or gardener in cash to be tax fraud? Why? Why not?
- Do you think some individuals and companies regard the government as fair game and tax evasion as a bit of a sport? What are the implications of this? How would you suggest tax crimes be prevented?

4. Violence, bullying and harassment

The culture of workplace management

The 1990s were characterised by significant workplace change and restructuring. Often this meant fewer people doing the same or more work. Longer hours, more responsibility, tighter deadlines, fewer resources, uncertainty about the future—all of this creates pressure. Sometimes the pressure can lead to anxiety, stress, tension and friction, particularly if the workload is not being shared equally or individuals do not have the skills or training to support their new functions. If issues are not dealt with, they may lead to conflict and not everyone has the skills to deal with conflict in a constructive way. Psychological research suggests that the incidence of aggressive behaviours tends to increase during periods of organisational restructuring and downsizing.⁹

Anecdotal evidence would indicate that organisations which are open, supportive, transparent in decision-making, displaying leadership and having clear lines of accountability and responsibility, tend to have fewer problems with conflict and violence. There are clearly implications here for human resource management strategies within organisations and imperatives for managers in the process of effective change management.

Professor John Toohey, Director, Office of Business & Technology, University of NSW, 'How can managers prevent the risk of occupational violence occurring within their organisations?' *Conflict and Violence in the Workplace* conference, Canberra, 23–24 April 1998.

Discussion starter

- In some work cultures, being able to cope with harassment and unreasonable work pressures is seen as a requirement to promotion. Have you ever heard comments like 'It's the way things are done', 'Do you want the job or not?' 'You've got to be tough to survive in a highly competitive market'? Do you agree? Is bullying inevitable at work?
- Have you been involved in workplace change or restructuring? How was it handled? Were particular individuals or groups targeted in the restructuring? Did it have an impact on levels of stress and aggression at work? Did it present a risk of violence?

Violence can come from within the workplace, as a result of an individual's actions, or part of a wider 'culture' of aggression within the organisation. It can also come from outside—a dissatisfied customer or client, an angry or hurt family member, a member of the public with a mental illness or a person committing a robbery. There is an emerging trend for particular kinds of violence outside the work environment, specifically domestic violence and stalking behaviours, to intrude into workplaces.¹⁰ But it is difficult to get a clear picture of the extent of workplace violence because it is not always reported and people use different definitions in their research.

There is general agreement that workplace violence includes things like homicides, rape, kidnapping, assault, robbery, threats, intimidation, obscene phone calls, harassment, including sexual harassment, stalking and damage to property. But what have the courts defined as workplace violence?

An Australian court has for the first time prosecuted a company and two of its directors under workplace safety laws over the sadistic 'initiation' of a teenage employee by other workers.

While courts have prosecuted employees for assault, companies have never been liable for prosecution under occupational health and safety laws.

NSW Chief Industrial Magistrate George Miller last week fined a joinery firm \$24,000 and two of its directors \$1000 each under the state Occupational Health and Safety Act—legislation normally reserved for workplace accidents.

Mr Miller said the company failed to adequately supervise or train its employees in health and safety and failed to 'prevent a premeditated act'.

Industrial relations lawyers say the decision could have wider implications for workplace bullying and could attract much higher fines.

In December 2001, 16-year-old asthma sufferer Dwayne Doyle had just started work at a family company, MA Coleman Joinery at Lidcombe in Sydney's west, when four colleagues attacked him and wrapped him in cling wrap from neck to feet.

His shoes and bag were then filled with sawdust and he was placed on a work trolley. The men then covered him with sawdust and squirted wood glue in his shoes, over his body and into his mouth.

‘Doyle, an asthmatic, coughed, choked and was unable to breathe,’ Mr Miller said. ‘What started out as a simple episode of bullying got out of control, leading to a serious physical threat to Doyle’s health and safety.’

Mr Miller said the employees were not disciplined, and director Brian Coleman knew an initiation would take place.

A second director, Graham Coleman, was supervising the factory floor on the day, but ‘his level of supervision did not deter these employees from carrying out their ceremony’.

Joe Catanzariti, a senior partner and head of workplace relations at law firm Clayton Utz, said the decision was ‘quite a revolution’.

Mr Catanzariti, who was on the NSW Law Society’s anti-bullying committee, said a bullying clause had been implemented into Victorian OHS legislation, but other states were yet to follow suit.

‘I think this is terrific—it sends quite a message to employers that they have a direct responsibility to provide a safe system of work and stamp out this sort of stuff,’ he said.

The Australian 10 May 2004

Discussion starter

- Is initiation something that happens in workplaces that you have had contact with? You might share your experiences.
- Do you believe there are any situations when bullying is appropriate at work?
- Break into groups of three or four and spend 10 minutes or so discussing your ideas about how bullying at work might be tackled.

Apprentice victim of ‘culture of abuse’

For a young Flynn [ACT] apprentice it was the workplace from hell. Robert Josifoski’s workmates filled his tool box, containing \$10,000 of his own tools, with oil, threw water over him, tried to give him electric shocks, and locked him in a cage.

Ten months of bullying led to the 22-year-old Josifoski accidentally hitting a colleague in the head with a hammer, the ACT Supreme Court heard yesterday. As a third-year apprentice mechanic at a Gregory’s Ford in Braddon, Josifoski was the victim of ‘nasty schoolyard behaviour’, including name-calling and pranks, inflicted on him by his more senior colleagues.

At farewell drinks for one of the men in February, a former employee of the car yard began calling Josifoski names and insulting his mother, continuing what Chief Justice Terence Higgins described as a ‘culture of abuse’ towards Josifoski. The court heard Josifoski tried to ignore the insults and had continued working. Josifoski said when he finished he went to wash his hands, which was when the victim told him he was going ‘to smash’ him. Josifoski said he was ‘really angry’ at that point, and grabbed a hammer out of his tool box. He went up to the victim to threaten him, however the hammer was greasy and slipped out of his hand, striking the victim in the head and causing a laceration, swelling and burst blood vessels in the right eye. ‘I wanted him to leave me alone so I could go home. I didn’t mean to hit him. There was no way in the world I

wanted him to get injured,' Josifoski said. Josifoski said he had not experienced such hostility before, except in Year Seven at high school, and that his managers ignored it and would 'walk away'. Josifoski's defence counsel, Shane Gill, described the bullying as having a 'nasty, schoolyard flavour', stating there was a 'tribal pecking order in the workshop and Mr Josifoski was very much at the bottom.'

Chief Justice Higgins criticised the behaviour of Josifoski's employers and colleagues. 'This sort of conduct is not permissible in a workplace,' he said. 'Their conduct cannot be justified. It is quite inappropriate for a workplace. One seriously wonders why management didn't do something about it before this incident occurred.' Josifoski pleaded guilty to assault occasioning actual bodily harm, but Chief Justice Higgins deemed the behaviour out of character and said Josifoski was 'completely unlikely to reoffend.' He placed him on a good behaviour bond for 12 months and said no conviction would be recorded if the bond was carried through. 'People can't be encouraged to pick up weapons and wave them at people because tragic consequences can and often do follow,' he said.

The Canberra Times 25 May 2004

Institutionalised abuse and initiation

Sometimes people may not recognise behaviour as violence and bullying because it is accepted as part of the 'culture'. This can be a particular problem in workplaces like the military, police services, or fire brigades.

'Initiation' or abuse of apprentices happens in other workplaces where there is hierarchy, a power imbalance or a culture that tolerates intimidation and violence. A NSW YouthSafe Committee member reports that a young bricklaying apprentice had his feet tied together to a bobcat and was dropped to the bottom of a hole where he was made to scoop water out of the hole with a bucket.¹¹

Discussion starter

- Have you ever experienced violence in your workplace or been in a workplace when a violent incident happened? If you feel comfortable, you might share your story. What were the circumstances? Was there any warning? Could anything have been done to prevent the incident?
- Were any steps taken to reduce the risk of future incidents?

Bullying

Workplace bullying can harm a person's well-being and lead to low morale or illness, become a significant drain on resources, reduce productivity and increase sick leave and WorkCover costs. It can also put employers and perpetrators at risk of legal action for negligence, breach of contract or breach of anti-discrimination or occupational health and safety laws or claims for unfair dismissal. Where bullying involves actual or threatened violence it becomes a crime.

Workplace bullying has been defined as 'the repeated less favourable treatment of a person by another or others in the workplace, that might be considered unreasonable and inappropriate workplace practice.'¹² It includes behaviour that intimidates, offends, degrades or humiliates a worker, possibly in front of co-workers, clients or customers.¹³

Workplace bullying can happen as part of an 'initiation' for new workers or apprentices. It can be the result of poor people management or communication skills. The pressures of restructuring and

'downsizing' can lead to demands for unreasonable performance or blaming an individual or group for the problems facing the organisation.

There is some evidence that workplace bullying is increasing. During July 2002–June 2003, the Queensland Working Women's Service received 4,192 general inquiries and handled 3,922 specialised assistance and case work inquiries. Workplace bullying issues accounted for 26.5 per cent of these inquiries.¹⁴

Discussion starter

- Not all bullying is a crime, even though it has serious consequences. Do you think there are forms of workplace bullying that should be regarded as a crime but are not at the moment?

Does bullying or violence happen in your workplace?

Workplace bullying is often not reported. People who have been bullied can often suffer from low self-esteem and start to believe that their behaviour causes the bullying. Cultural constraints may stop someone from raising their concerns, or they may feel powerless because of their position in the organisation. Other things that make reporting difficult include a 'don't do' culture, embarrassment, anger, frustration and fear. But there might be other signs of trouble that suggest bullying or violence is a problem:

- a high rate of 'sickies'
- high staff turnover or sudden, unexplained resignations (particularly among apprentices and junior staff)
- women who don't come back from maternity leave but do go on to work somewhere else
- a high level of stress-related sick leave
- a significant drop in morale or productivity.

What are the risks?

This section draws on a presentation by Dr Greg Ash, Manager, Policy and Labour Regulation for ACT WorkCover at the *Conflict and Violence in the Workplace* conference, Canberra, 23–24 April 1998.

Workplace violence can happen anywhere and affect anyone. But some workplaces are at greater risk than others. They include financial institutions and other places where substantial amounts of cash are held, or where cash might be easily accessible (say at all-night service stations where only one person is working), places where drugs are held or shops that stock goods which are readily re-sold, and licensed venues, particularly pubs.

Some occupations also face an increased risk of violence at work: police, prison officers and other security personnel, bank and building society staff, petrol station and pharmacy workers, liquor store staff, taxi drivers and nurses.

What kinds of factors put people at increased risk?

- contact with the public, particularly receiving complaints and dealing with money—for example, health care agencies, social and welfare services, the hospitality industry, public safety and enforcement agencies
- delivering passengers, goods or services
- duties that include control or enforcement
- a mobile workplace or one that is in a high crime area, working with unstable or volatile

people, working alone and working at night.

The environment—how a workplace is built and organised—can also affect risk levels. Workers may be at greater risk if the public has easy access to employees, if the workplace and areas around it are poorly lit or if it is hard for other staff to see or hear if assistance is needed. Poor management and inadequate training can also put people at increased risk of violence. The incidence of aggressive behaviours is generally higher in workplaces with a negative organisational climate and low staff morale.¹⁵

Discussion starter

- Does anyone in the group work in a high-risk industry? What does the business or organisation do to prevent or reduce the risk of violence? Have you got any practical suggestions that might strengthen current arrangements? What would it take to get your ideas implemented?

What makes someone violent at work?

Research suggests that certain types of people are more likely to commit violence at a workplace:

- the angry customer/service user
- the mentally ill person
- the aggrieved party in a domestic dispute
- the criminal
- the disgruntled employee.¹⁶

Research also suggests some common factors that contribute to workplace violence:

- feeling aggrieved
- being forced to wait
- perceived intrusions into private life
- prejudice
- negative/intolerant staff attitudes
- substance abuse
- personality instability.¹⁷

Working in particular industries can also contribute to the risk of experiencing violence at work, as demonstrated in a recent report funded by the Criminology Research Council on violence, threats and intimidation against child protection professionals.¹⁸

Discussion starter

- Would you add anything to the factors mentioned in the two lists above?
- Alcohol plays a major role in violence in Australia. The problems that come with being drunk can be made worse in crowded and uncomfortable circumstances. In your experience, is violence a problem in pubs, clubs or other licensed venues in your area?

Violence in retail premises

In 2003, over 23 per cent of robberies occurred in retail premises.¹⁹ (Robbery is the unlawful taking of property without consent, accompanied by force, threat of force or violence and/or putting the victim in fear. Armed robbery is robbery with a weapon.) 36 per cent of robberies involved the use

of a weapon.²⁰

Improved security, particularly by financial institutions and some government agencies, has meant a greater focus on 'softer' targets like service stations, milk bars and 24-hour convenience stores. The increased use of credit and debit cards rather than cash, as well as security cameras, has also shifted the focus from major retail outlets to smaller stores and those that deal mainly in cash.

Discussion starter

- Have you or anyone you know had experience of armed robbery? What was the story? Was any action taken to reduce risk? Was ongoing support or counselling provided for those involved?
- Is armed robbery a particular issue in your community or workplace? Do you know what is being done to address the problem, or could you find out? Are there ways that your group could work in partnership with others, such as law enforcement agencies, local government and chambers of commerce, to help address the issue?

Prevention strategies

Sometimes very simple strategies can increase the effort involved in committing the crime to a point where it is no longer worthwhile. For example, an up-market women's clothing store had tens of thousands of dollars worth of stock on its racks but foiled an attempted robbery by having every second coat hanger facing the opposite direction—increasing the effort and the time involved for the potential robber.²¹

Adam Graycar, former Director of the Australian Institute of Criminology, suggested the following list of robbery reduction strategies on the basis of studies over the past 20 years:

- two or more assistants
- good cash handling
- concealed access eliminated
- locate store near evening commercial activity
- exterior visibility enhanced
- store closed from 10 p.m. to 6 a.m.
- security devices in use
- cashier located in security enclosure
- employees trained in prevention
- interior visibility enhanced
- petrol pumps present in front of store
- cashier located in store centre
- store on busy street with heavy traffic
- security guard on premises.

The National Crime Prevention Program has published a crime prevention kit for small business. It is available on the Internet at <http://www.crimeprevention.gov.au>.

What's your advice?

A couple in their 60s own and run a small shop. They are held up and robbed at gunpoint. The business is located in a suburb well known for high rates of drug dealing and drug-related crime and had been held up several times before the couple bought it. During the robbery the male owner was forced to open the

safe with a gun pointed at his head. He thought during this time that he would get the combination to the safe wrong and was sure the perpetrator would shoot him. Once the safe was open and the money taken, the perpetrator left the shop.

The chances of being robbed again are extremely high. The owners do not have regular help to draw on and are under high levels of stress. The nature of their business makes it impossible to install protective screens. The couple contacts your group for advice about what they should do. What suggestions would you make?

Safety and the home

Changing technology, an increase in contracting out and consultancy work, and the major growth in the number of small businesses run by women has meant a significant increase over the past decade in the number of Australians who work from home. As of June 2000, 980,300 people aged 15 and over were employed at home (meaning they worked all or most hours at home (692,600) or employees who had an arrangement with their employer to work some hours at home, in their main or second job (287,700)). This represented 11 per cent of all employed people. Women made up just under half (49%) of those employed at home.²² The extent of domestic and family violence in Australia (see the *Personal Violence* module) suggests that the workplace of some of these women is unsafe.

For many women the home is the primary workplace for some part of their life although that work is usually unpaid. Even women in the paid workforce still do 70 per cent of the unpaid work in the home.

While people working from home may avoid some of the risk factors associated with other workplaces, isolation, being away from public scrutiny or the lack of mechanisms to resolve conflict are factors that may increase risk.

Discussion starter

- Is your home also a workplace? How safe is it?
- What might be done to reduce the risk of violence?

Preventing workplace violence

You can never stop all violence and bullying. But you can take steps to help prevent foreseeable harm in the workplace and protect the organisation from liability for the wrongs of others. In the [*Additional Resources*](#) at the end of this module you will find some suggestions about steps to prevent violence, bullying and harassment, and ways to handle them if they happen.

Developing a policy is not hard. But it will only work if it is consistently implemented, taken seriously and reviewed regularly. You may need to think about training people in the organisation in how to resolve conflicts and avoid violence. There is usually something you can do to influence a potentially violent situation, but it generally requires good personal skills.

A key part of prevention is tackling the underlying causes of violence, not just dealing with its effects. If you are interested in helping your workplace minimise the risk of violence or bullying, there is a range of tools that may help. You will find some suggestions at the end of the module.

5. Fraud and deception

Fraud basically means using dishonest means to get financial or other benefits or to injure the rights or interests of another person or organisation. Fraud itself is not treated as a specific crime in Australia, apart from conspiracy to defraud; various property offences, including theft and obtaining a financial advantage by deception, are used to prosecute fraudulent or dishonest conduct.

Common types of fraud include credit card fraud, identity fraud, insurance and bank fraud and telecommunications fraud. Bankruptcy and fraud are also linked; sometimes people fail to disclose assets, incur a debt without expectation of being able to pay, obtain credit or incur a liability without disclosing bankruptcy, or transfer property to someone so creditors can't get to it.

People who commit fraud rely on ignorance and trust, and on the fact that some people don't take the time to check out whether a claim is legitimate. For example, the Serious Fraud Investigation Branch of the Australian Federal Police regularly receives complaints from businesses that have received invoices from publishers of small, obscure out-of-state publications, requesting payment for advertisements allegedly placed in their magazines or papers. When queried about an invoice, the publisher generally adopts an aggressive attitude stating the debt will be referred to a debt collector or placed before the courts.

A range of public and private agencies now holds large amounts of information about us on computers. With the growth in the use of credit and debit cards, information technology is making it possible to put together a detailed picture of our personal preferences by analysing our buying habits. There is also a greater opportunity to access or interfere with confidential and personal information. Breaches of privacy and improper disclosure and use of information, including for bribery or defamation, are likely to become increasing problems in the future.²³

Discussion starter

- How much emphasis should the community and governments give to crimes with a big financial impact, such as fraud, compared with those that involve substantial personal or social cost?

Corporate fraud

According to the 2002 Australian and New Zealand Fraud Survey conducted by the company KPMG, the cost of corporate fraud more than doubled in the two years since its previous survey. At a conservative estimate, approximately 360 of Australia's and New Zealand's top 2,000 companies have lost more than \$27.3 million in fraud since the 1999 survey, and the researchers say the figure is only the tip of the iceberg. According to KPMG, the average cost of fraud per organisation increased from \$1.1 million to \$1.4 million. The overriding of internal controls was the most significant contributing factor.

Non-management employees were responsible for 72 per cent of internal fraud, involving theft and misappropriation of funds. Management committed 28 per cent of internal fraud, most of which involved misappropriation of funds.

Discussion starter

- According to the author of the KPMG survey, the same types of fraud are a problem in each survey. 'They are the same things over and over, and they are things people can deal with, so why aren't they doing something about it?' What's your response?
- In your experience, what does it take for an organisation to take fraud seriously?

- Has anyone in the group had experience of fraud at work? If you feel comfortable, you might like to share your story.

Reducing the risk of internal fraud

Good administrative, managerial and audit procedures will help prevent fraud. So will education and training for staff to motivate them to reduce the potential for fraud. But sometimes it can be hard to take all the necessary precautions. In very large businesses, it may be easy to hide small-scale fraud. Small business people may feel they don't have the time or the expertise to set up systems to minimise the potential for fraud. In a small, busy shop, for example, you might see a range of things that increases risk:

- inadequate supervision of staff
- limited or unclear separation of duties between staff
- inadequate training of staff
- use of common cash registers, cash drawers etc. among staff, making it hard to pinpoint responsibility for any discrepancies
- large amounts of cash kept on hand and infrequent banking
- poor banking procedures
- poor cash handling and reconciliation procedures.

Discussion starter

- Has anyone in the group had experience of fraud? What were the circumstances? What was the outcome, including the impact on the business and individuals? Was anything done to reduce future risks? Was the problem hard to deal with?
- If this is an issue that concerns you, you may want to ask your state or territory police if they can provide or recommend someone to talk with your group. Alternatively, someone in your group or a local service club like Rotary may know a person with experience in the area and who would be willing to talk to the group.

If you're interested in looking further at this issue or want to improve procedures in your workplace, business or club, you can find some useful tips in the NSW Police Fraud Enforcement Agency's *Guidelines to Fraud Prevention*. It can be accessed via the Internet at <http://www.police.nsw.gov.au/prevention/prevention.cfm>.

Superannuation fraud

The Superannuation industry has over \$495 billion in funds invested.²⁴

Super Fund Foils \$150m Sting

A sophisticated \$150 million attempted fraud on one of Australia's largest superannuation funds, the \$5.5 billion Commonwealth Superannuation Scheme, has raised concerns about the use of faxes to transfer funds rather than the more secure electronic transfer systems.

The near-miss gave weight to concerns by the Australian Prudential Regulation Authority, which last week highlighted the case.

The attempted fraud was narrowly averted last Christmas by the custodian, J P Morgan Chase, which received a fax late on Christmas Eve asking that \$US112 million (then

worth \$150 million) of funds in three CSS accounts in Switzerland, Hong Kong and Greece be transferred.

A Morgan officer took action on the requests. On Boxing Day further checks by systems operating for overseas clients who do not take Christmas off revealed the fraud.

Immediate action managed to claw back most of the money while it was still within the banking system and the CSS account was restored by JP Morgan in a short time.

Custodians operate as the guardians of money and securities held by funds and fund managers on behalf of fund members.

The fraud is still being investigated by Australian Federal Police, who are believed to have said they had not previously seen anything as sophisticated as the scam.

‘Superannuation is a big industry and the more money involved, the more people will try to get at it,’ CSS chief executive Steve Gibbs said yesterday.

He said the incident showed that the system to prevent fraud was working, a comment echoed by a spokeswoman for Finance Minister Nick Minchin in saying no legislative change was required.

Details of the attempted fraud were revealed on the Nine Network Sunday program yesterday and confirmed by CSS and J P Morgan.

APRA General Manager Diversified Institutions, Ramani (S G) Venkatramani, cited the case last Tuesday as a lesson for super funds to choose their service providers carefully.

He said that in one case the custodian ‘received instructions late in the day on Christmas Eve over [the] telephone, followed by faxes to remit substantial funds to overseas accounts never used before. The officer concerned actioned the requests without performing the requisite return confirmations, and after Boxing Day further checks revealed the fraud’.

While J P Morgan Chase disputed the phone claim, 20 per cent of transfers in the superannuation system use telegraphic transfers and notifications using faxes. The rest are made through an electronic system owned by leading banks or the major custodians’ proprietary web-based systems.

Australian Financial Review 7 June 2004

Discussion starter

- Do you think enough attention is given to ‘white-collar crime’?
- Do you know what safeguards your superannuation fund has in place to minimise the risk of fraud or misuse of money? Where could you find out?

Fraudulent investment schemes and financial scams

‘Hello, this is Jim from the ABC Bank. We have had trouble with the bank’s computer systems, so to protect your funds we are going transfer all your money to a special bond account. In order to transfer the money I will need to get your bank account details and a

verbal authorisation to transfer the funds ...’

‘Hello this is Bonnie from Smartercard. In order to make your credit card compliant with our new system we are going to send all our customers a sticker that you will need to affix to your card. So can I just have your credit card number for verification?’

The Little Black Book of Scams: A Consumer’s Guide to Scams, Swindles, Rorts and Rip offs.

It’s estimated that more than 100,000 Australians have lost money in fraudulent and illegal investments in the past 10 years. Financial fraud can range from elaborate hoaxes that get people to invest in non-existent schemes through to theft of money from a cash register, or falsification of cash receipts.

As businesses in the public and private sectors rely more and more on technology, new opportunities for fraud emerge. The growth of electronic commerce will create possibilities for significant fraud in cyberspace. Increasing fraud is expected in the areas of consumer, identity, currency, plastic card, superannuation, public sector, and telecommunications, as well as cyber-fraud and other computer-related fraud.²⁵

The Internet has revived old scams such as chain letters, unsolicited business or investment offers and pyramid schemes. In a typical pyramid scheme a potential member is asked to pay to join the scheme. The only way to advance is to recruit others, who also pay to join. If enough new members join, the pyramid grows, but in order for everyone to profit there must be an endless supply of newcomers. In reality, each new participant has less chance of recruiting others and a greater chance of losing money. In Australia it is illegal to promote or participate in a pyramid selling scheme. Penalties include fines of up to \$200,000 for a company or \$40,000 for individuals. The Internet makes it easy for fraudulent operators to hide, shut down or move on. Clever web-sites may look legitimate and be more convincing than newspaper advertisements making the same false claims.

Internet scam

An Internet banking scam that duped Australian bank customers into giving passwords to fraudsters could have been the work of a global syndicate, according to a British internet security firm.

The Mi2g Intelligence Unit, which monitors global hacking activity, lists Australia’s five largest banks among 13 banks and five e-commerce websites hit by ‘phishing’ scams in recent months. St George Bank customers were caught by the scam a few weeks ago.

Britain’s Barclays Bank said last week that 400 customers had reported a similar scam and a ‘handful’ of customers had been duped into sending account details to a fake bank security site.

Another British bank and two Canadian banks were also on the list, as were Amazon.com, AOL, Best Buy, eBay and Paypal.

The modus operandi is always similar: customers receive an email that appears to come from the bank or commerce site asking them to click on a link, supposedly to a secure site, where they are asked to update their passwords and personal details. The emails and bogus websites closely mirror the legitimate site’s own branding.

St George said fewer than five customers were affected, with total losses of about

\$10,000. Earlier in the year, eight Commonwealth Bank customers had \$27,840 taken from their accounts.

The executive chairman of mi2g, D K Matai, said the 'elaborate nature of this scam covering three continents over the last few months suggests the hand of one or more global crime syndicates.

'This is a global crime being perpetrated with precise local knowledge of which online banking customers are to be targeted specifically.'

The director of the Australian Bankers Association and co-ordinator of the ABA Fraud Taskforce, Tony Burke, agreed the scams 'exhibit a high degree of sophistication . . . We've moved well past the Nigerian scam letter'.

The Australian internet banking customers who lost money through such fraud have been reimbursed by their banks.

The Sydney Morning Herald 18 September 2003

ASIC has a *consumer website* <http://www.fido.asic.gov.au/> that provides information on things such as investment schemes designed to help minimise tax and provides advice to help reduce your risk of being ripped off and losing your money.

Police Bust Fake ID Scam That Netted \$1m

An identity fraud ring targeting Sydney Koreans allegedly obtained hundreds of fraudulent bank loans, luxury cars and mobile phones worth more than \$1 million.

Police arrested six people yesterday after simultaneous raids by 40 fraud squad detectives on homes in Eastwood and Epping.

Bundles of fake drivers' licences, embossing machines and computer equipment used to create false Medicare cards and other documents were seized.

Police said ads in Korean-language community newspapers offered up to \$500 to recruit students on temporary visas, or visitors who had overstayed visas, to 'lend' their identity and walk into banks and phone dealerships for a small percentage of the gains. Others were paid simply to have their photograph taken.

Detective Inspector Mike Edgton, of the state Crime Command Fraud Squad, said the syndicate had been running for at least three years. Information from banks sparked the investigation several months ago.

Five of those arrested were Korean nationals and the other was an Australian.

Police believe two of the men are the syndicate's organisers. They could face charges of use and possession of a false instrument and up to 10 years in jail.

Police said they would work with the Korean Society of Sydney to raise awareness of the scam, and to locate others who may have unwittingly taken part.

A meeting of local Korean media was held last night. A daily and four weekly newspapers and six magazines compete in Sydney.

The general manager of the Korean Society, Sang Doo Ok, said most publications were aware of the problem with the ads and did not run them, but some had.

Mr Ok said most of the people paid by the syndicate for photographs were visitors to Australia on tourist or business visas.

The Australian Bankers' Association fraud taskforce has proposed an online gateway to link banks with government departments that issue identity documents so they can be instantly verified as authentic on presentation in a bank branch.

Feasibility studies are due by October from the federal government and the banking industry.

The ABA's director, Tony Burke, said it was banks that typically 'wore the loss' on identity theft cases, and they were seeking to tackle the threat on a number of levels.

The banking industry is developing standards for passwords and guarding pin numbers, such as shields to be installed on Eftpos devices so entry cannot be observed.

But Mr Burke said raising security standards would not wipe out identity fraud.

'It is not just the technology that is key, but the processes,' he said. 'If an ID is issued wrongly in the first place it is not achieving anything.'

The Sydney Morning Herald 13 August 2003.

Discussion starter

- To date, regulating and controlling what is available on the Internet has proved difficult. How do you think undesirable Internet-related activities should be tackled?
- Have you had any experience of financial fraud? What were the circumstances? Could anything have been done to prevent it? What did you learn from the experience?

Reducing your risk of being ripped off

People in a hurry, people who are trusting and don't take the time to check information for themselves, people who are frail or dependent on others for advice on financial matters—these are the sorts of people who may be vulnerable to fraud.

The best defence against scam operators is information and caution. You are less likely to be caught by a fraudulent scheme if you do some homework—like checking up on the background of those putting it forward.

Activity

- You are looking for ways to reduce your tax bill at the end of the financial year. You see an advertisement calling for investment in a plantation of trees that contain a newly discovered chemical that helps people lose weight. It is promising a good rate of return, tax-free. You are running out of time to check the details of the proposal. Should you consider investing some money? What are the most crucial things you

need to do to ensure the proposal is legitimate and to minimise your risk?

- Break into small groups and brainstorm some ideas about the questions you need to ask and where you might go for answers. If you want some help, have a look at the case study in the *Additional Resources* at the end of the module.

Who commits fraud?

In the June 1999 issue of the UK-based publication *Fraud Intelligence*, an article by Dr Raj Persaud, a consultant psychiatrist at the Bethlem Royal and Maudsley Hospitals, looked at the type of person most likely to attempt fraud. The article included a test for people to check their own personality. It is reproduced below.

Test yourself

Each statement is followed by two possible responses—agree or disagree. Read each statement carefully and decide which response best describes how you feel. If you are not sure which response is more accurate, choose the one you feel is most appropriate. Don't spend too long on each statement. When you have finished, check your responses against the assessment below.

Questions	Agree	Disagree
Good behaviour is usually rewarded.	A	B
It is better to impress than to be good.	B	A
The world is largely a just place.	A	B
Charm counts for more than skill.	B	A
I am generous towards my competition.	A	B
I will look for any advantage I can get.	B	A
Most people do not try to cheat.	A	B
An admission of guilt should be rewarded.	B	A
Winning is not everything.	A	B
Success is rarely about hard work.	B	A

Discussion starter

- According to Dr Raj Persaud, the more Bs you score, the more likely you are to be a financial psychopath. You are also more likely to be a high flyer.
- Break up into small groups and discuss your results. Do you agree with the idea that some types of people are more likely to commit fraud? Do you think the level of economic competition today increases the risk of fraud?

6. Fraud against government

The Australian Government, state and territory, and local governments collect and spend a large amount of money—billions of dollars. Fraud against the government can come from inside—from employees or contractors—or from the public, by accessing payments they are not entitled to or failing to make payments that are due such as income tax. But fraud is not restricted to monetary or material benefits. Other benefits that could be fraudulently sought include rights of entry to Australia, documentation conferring identity such as a passport or birth certificate, or information.

The nature of what governments do means that preventing fraud is not just about avoiding financial loss but also about avoiding damage to its security or integrity, avoiding harm to the economy,

resources, assets, environment or well-being of Australia, and protecting the public interest.

Risk factors

In terms of internal fraud, governments face some of the same risks as private sector organisations. As with the private sector, prevention is the best approach, including by identifying those functions that can pose a particular risk of fraud:

- outsourcing and grants programs
- use of government credit cards
- travel allowance and other common allowances
- purchasing
- physical security
- computer security
- salaries
- property and other physical assets.

As the business of government changes and technology makes possible new ways of committing fraud, new approaches to managing risk are needed.

Discussion starter

- Occasionally you hear of whistleblowers who have reported inappropriate behaviour in an organisation and then find themselves persecuted for speaking up. Do you know of situations where someone has been punished for 'doing the right thing'? What were the circumstances? Why did the organisation react the way it did?
- Sometimes people don't report wrong-doing because they fear they may lose their job. How could organisations be encouraged to take a more constructive approach to individuals who point out problems in the organisation?
- There have been calls to pass laws that protect whistleblowers. Do you think this would be useful? Or would it just protect troublemakers?

Welfare fraud

The Australian Government, through Centrelink, provides a wide range of support and safety net services. One of Centrelink's responsibilities is to ensure that people receive no more or less than what they are entitled to. Review and compliance activities are a major part of this, with 4.4 million reviews of social security payments conducted each year. In the 2002–2003 financial year:

- 835,398 payments were either cancelled or reduced as a result of Centrelink compliance activities. This resulted in more than \$419.9 million in welfare debt which debtors were required to pay back.
- 2,853 convictions were recorded for welfare fraud involving over \$31.1 million.

Compliance mechanisms include data-matching, obtaining information from other agencies or the public, and regular payment checks.

Data matching involves comparing customers' identity details with the records of other Australian Government and state bodies to identify income or changes in circumstances that customers had not declared. For example, comparing Centrelink data with Australian Taxation Office Employment Declaration Form data can identify customers who have not declared income received from employment. Comparing Centrelink data with immigration records identifies customers or their

children who are not residentially qualified for welfare payments.

Discussion starter

- Do you see welfare fraud as a big problem? Is it an issue in your local area?
- The Australian Government can access a wide range of information about people who receive payments from Centrelink. Do you think we have the balance right between avoiding fraud and protecting privacy?
- If your group is interested in looking further at welfare fraud, you might research how the penalties for welfare fraud compare with those for, say, tax fraud or corporate fraud. Are the penalties similar for similar amounts of money?

Wind-up

The last part of each learning circle session is an opportunity to reflect on what has been learnt, evaluate how the session has gone, and allocate any tasks the group agrees need to be done before the next session. You might find it useful to sum up your discussion under the following headings:

Difficult points

- Are there any areas where you need more information? You might like to invite a guest speaker or find more information from an expert group or government department. Don't forget local libraries, community groups and the Internet.
- Briefly summarise those areas where you have agreed to disagree. This will identify minority views as still being valid.

Decisions

- Is there anything that the whole group has decided about your discussion?
- Is there anything you would like to do differently next time?
- Did you achieve what you had hoped?
- Is there any other action you want to take? This might include contacting your local council or politicians about an issue the group thinks important, or watching a video.

Finally

- Continue to collect articles from local media on issues that concern you.

Additional Resources

1. Doing something about workplace bullying

From Workplace Bullying: An Employers' Guide, Division of Workplace Health and Safety, Department of Employment, Training and Industrial Relations, Queensland Government, in conjunction with the Australian Council of Trade Unions, the Queensland Chamber of Commerce and Industry and the Queensland Working Women's Centre.

It may not be possible to remove all sources of bullying from the workplace. However, in consultation with workers, you should manage existing and foreseeable sources of bullying by:

- finding out if bullying exists at your workplace
- developing and implementing a plan to minimise workplace bullying, in consultation with workers, including:
 - policy
 - contact person
 - procedure
 - training and education
- reviewing the strategy.

The involvement of workers and managers will help to encourage a commitment to managing bullying in the workplace. It may be useful to include workers who have experienced bullying at work in the consultation.

The strategy could be included in an existing policy/procedure, such as an anti-discrimination policy/procedure or grievance policy/procedure. An example policy is set out at in the booklet *Workplace Bullying: An Employers' Guide* and can be downloaded from the Internet www.qld.asu.net.au/health&safety/fs_bullying.php

2. What to do if you are bullied or see bullying at work

From the website of the Queensland Nurses' Union, in association with the Australian Nursing Federation (Qld Branch).

- Raise the issue at staff meetings so that people are aware of the issue.
- Ensure your area or workplace has a procedure in place for dealing with this issue.
- All Awards have a Grievance Procedure which may be modified to deal with bullying. The Queensland Nurses' Union does not advocate introducing new systems into the workplace on this issue.
- Your workplace may have a Sexual Harassment Referral Officer or Workplace Health and Safety Representative network that could be modified to incorporate assisting people with bullying issues. However, people who will be required to deal with bullying should have appropriate training on this issue.
- The workplace should have a clear statement indicating that bullying is not acceptable and outlining the types of behaviours that are to be regarded as inappropriate.
- Should you be subjected to bullying, take comprehensive notes regarding the incidents—this can be in diary form. Should your health deteriorate due to this behaviour, you may be able to claim WorkCover.
- If you witness such behaviour, in some instances immediate intervention may be appropriate, or there may be the need for an incident report to be written. Access to appropriate counselling services should also be available in the workplace for staff involved in these issues. Some contacts are:
 - Queensland Working Women's Service, *Workplace bullying factsheet*
Includes a checklist, 'What can you do?'
http://www.qwws.org.au/pdf_Files/bullying.pdf
 - South Australian Office of the Employee Ombudsman 1999, *Bullies not wanted: recognising and eliminating bullies*
Includes chapters about reporting workplace bullying, guidance for victims, and where to go for advice, information and assistance.
<http://www.employeeombudsman.sa.gov.au/info/>

3. Tips for avoiding financial fraud or shonky investments.

There is a list of ways to protect yourself on the scamwatch site at http://www.scamwatch.gov.au/content/investment/financial_py.asp

From *The Little Black Book of Scams: A Consumer's Guide to Scams, Swindles, Rorts and Rip offs*

http://www.consumersonline.gov.au/Content/publications/consumer/resources_black_book.asp

- Make sure that an investment opportunity and the person or company promoting it are properly registered with the Australian Securities and Investments Commission (ASIC).
- Check out the company or individual's track record with your state or territory consumer affairs or fair trading agency or the Australian Securities and Investments Commission.
- Take your time. While there may be time limits for special offers, high-pressure sales tactics are often danger signs of a scam.
- Remember that people in cyberspace are not always what they seem.
- Don't expect to get rich quick, and invest only with those you know and trust.
- Don't assume that your online computer service polices its investment bulletin boards.
- Don't buy thinly traded, little known shares strictly on the basis of online hype.
- Don't give your bank account numbers, credit card numbers or other personal information to anyone you don't know or haven't checked out.
- Don't judge reliability by how professional a website looks. It's easy and costs very little to create, register, and promote a website.
- Don't accept unsolicited e-mails. Scam artists often use them.

More information

Crimes against businesses

Australian Government, National Crime Prevention Program, 2004

- *Small business—is your business secure? A crime prevention kit for small business*

- *E-crime: a crime prevention kit for small business*

Available at <http://www.crimeprevention.gov.au/> or phone 1800 708 777.

Australian Institute of Criminology, *Retail and small business crime*

<http://www.aic.gov.au/topics/business/>

Most state and territory police services produce a range of crime prevention brochures, pamphlets, stickers etc. Some of these address crimes against business

ACT Policing, *Business security awareness*

Information on understanding and minimising business crime, fraud, robbery and theft,

<http://www.afp.gov.au/page.asp?ref=/Prevention/SafetySecurity/BLOfficer/SecurityAwareness/>

South Australia Police, *Business Crime*

http://www.police.sa.gov.au/crime/crime_reduction_section/business_crime.shtml

The Queensland police service has produced a detailed booklet called *Business Security* which covers things like environmental design strategies, risk, safes, cash handling, moving cash, meeting potential threats and combating theft by employees. It is available to read or download from their website:

<http://www.police.qld.gov.au/pr/services/infopks/>

City of Unley (SA), *Retail crime prevention fact sheets*

<http://www.unley.sa.gov.au/site/page.cfm?u=346>

Other organisations and documents you may wish to consult for further information include:

Australian Securities and Investments Commission, <http://www.asic.gov.au/>

Australian Crime Commission, <http://www.crimecommission.gov.au/>

Workplace violence and bullying

Australian Institute of Criminology, *Occupational violence*
<http://www.aic.gov.au/research/cvp/occupational>

Beyond Bullying Association
<http://cwpp.slq.qld.gov.au/bba/>

Mayhew, C 1989-2003, *Occupational violence in Australia: an annotated bibliography of prevention policies, strategies and guidance materials*
<http://www.aic.gov.au/research/cvp/occupational/bib.html>

Queensland Government Workplace Bullying Taskforce 2002, *Creating safe and fair workplaces: strategies to address workplace harassment in Queensland*
<http://www.whs.qld.gov.au/taskforces/bullying/bullyingreport.pdf>

South Australia Office of the Employee Ombudsman 1999, *Bullies not wanted: recognising and eliminating bullying in the workplace*
http://www.employeeombudsman.sa.gov.au/info/Bullies_not_wanted.htm

Worksafe Victoria 2003, Prevention of bullying and violence at work : guidance note
Available at <http://www.workcover.vic.gov.au/>

A secure workplace for young Australians is a project of WorkCover NSW and the National Children's and Youth Law Centre. A number of publications have been produced for the project, including *Prevention Strategies for Your Business*, *Intervention Strategies for Your Business* covering steps that must be taken when workplace violence, bullying and harassment are identified or suspected.

Fraud and computer-related crime

Australian Government National Crime Prevention Program website
<http://www.crimeprevention.gov.au/>

Australian Government ScamWatch website
<http://www.scamwatch.gov.au/>

Australian Institute of Criminology, *Cybercrime*
<http://www.aic.gov.au/topics/cybercrime>

Australian Institute of Criminology, *Fraud and white-collar crime*
<http://www.aic.gov.au/research/fraud/>

Smith R G 1999, 'Fraud and Financial Abuse of Older Persons', *Trends and issues in crime and criminal justice*, Australian Institute of Criminology, October 1999. [or, a more recent Trends & Issues paper:] Muscat, G, James, M & Graycar, A 2002, *Older people and consumer fraud*
<http://www.aic.gov.au/publications/tandi/tandi220.html>

The Australian Federal Police publishes *COMFRAUD Bulletin* four times a year. It provides information on fraud-related developments and can be accessed on the Internet:
<http://www.afp.gov.au>.

The Australian Securities and Investments Commission is responsible for consumer protection in financial products covering superannuation, life insurance, general insurance and deposit taking (but not credit). A range of useful information can be accessed through its website, <http://www.asic.gov.au>.

See also ASIC's consumer website, *FIDO*, <http://www.fido.asic.gov.au/>

The Little Black Book of Scams: A Consumer's Guide to Scams, Swindles, Rorts and Rip offs describes the many frauds, scams, rorts and rip offs used by swindlers to gain trust and acceptance, and ways that consumers can protect their hard-earned dollars. The publication was an initiative of the Ministerial Council on Consumer Affairs and marked 1999, the International Year of Older Persons. It is available on the Internet at http://www.consumersonline.gov.au/Content/publications/consumer/resources_black_book.asp (Fourth edition, February 2004).

Notes

1 Dennis Challenger, 'The realities of crime against business', AIC Crime Against Business Conference, 18–19 June 1998, quoting examples from K. Sibley, 'Piracy Message Short-Circuiting', *Computing Canada*, 30 March 1998.

2 Business Software Alliance & IDC 2004, First Annual BSA & IDC Global Software Piracy Study. Business Software Alliance: Washington DC.

3 'Fake Mice cost \$200,000 a month', *Handbook of Security* Supplement 55, 1997, Kluwer, Amsterdam, pp. A-18.

4 See the Victorian Environment Protection Authority's website at: www.epa.vic.gov.au/industry/ChangesToTheAct/default.htm.

5 See the New South Wales Environment Protection Authority's website at: www.epa.nsw.gov.au/small_business/composites.htm.

6 See the Environment Protection (Sea Dumping) Act 1981 as amended by the *Environment and Heritage Legislation Amendment Act 2000, No. 107, 2000*.

7 Pain, Nicola, 'Criminal law and environmental protection: overview of issues and themes', Australian Institute of Criminology conference on *Environmental Crime*, 1–3 September 1993.

8 Fisse, B and Braithwaite, J. (1988) 'The allocation of responsibility for corporate crime: individualism, collectivism and accountability', *Sydney Law Review*, vol. 11, no. 3, pp. 468–513.

9 Dr Peter Cotton, Clinical Psychologist, 'Preventing Workplace Violence', *Conflict and Violence in the Workplace* conference, Canberra, 23–24 April 1998.

10 Dr Peter Cotton, Clinical Psychologist, 'Preventing Workplace Violence', *Conflict and Violence in the Workplace* conference, Canberra, 23–24 April 1998.

11 Lynda Bennett, YouthSafe Committee Member, 'NSW Labor Council YouthSafe Program', *Conflict and Violence in the Workplace* conference, Canberra, 23–24 April 1998.

12 *Workplace Bullying: An Employer's Guide*, Division of Workplace Health and Safety, Department of Employment, Training & Industrial Relations, Queensland Government.

13 *Workplace Bullying*, Queensland Nurses' Union, in association with the Australian Nursing Federation (Qld Branch).

14 Queensland Working Womens' Service Inc. (1997) *Annual Report*, Brisbane.

15 Dr Peter Cotton, Clinical Psychologist, 'Preventing Workplace Violence', *Conflict and Violence in the Workplace* conference, Canberra, 23–24 April 1998.

16 Peter Jones, Manager Corporate Assessment Services, Davidson Trahaire, Sydney: presentation on 'Identifying the risks', *Conflict and Violence in the Workplace* conference, Canberra, 23–24 April 1998.

17 Hoad, C.D., (1993) 'Violence at work: perspectives from research among 20 British employers', *Security Journal*, 4, 64–86; cited in Dr Peter Cotton, Clinical Psychologist, 'Preventing Workplace Violence', *Conflict and Violence in the Workplace* conference, Canberra, 23–24 April 1998.

18 Freda Briggs, Donna Broadhurst and Russell Hawkins (2003). Violence, threats and intimidation in the lives of professionals whose work involves child protection
<http://www.aic.gov.au/crc/reports/200102-15.html>

19 ABS, *Recorded Crime Australia* 2003, released May 2004,.

20 ABS, *Recorded Crime Australia* 2003, released May 2004, .

21 Adam Graycar, Director, Australian Institute of Criminology, *Conflict and Violence in the Workplace* conference, Canberra, 23–24 April 1998.

22 Australian Bureau of Statistics 2001, *Locations of Work June 2000*. CAT no.6275.0, ABS: Canberra.

23 Queensland Working Womens' Service Inc. (2003) *Annual Report 2002/2003*, Brisbane.

24 Smith, R G 1998, *Criminal exploitation of new technologies*, Trends and Issues in crime and criminal justice, No. 93, Australian Institute of Criminology, p.4.

?? AusCERT 2002, *Australian Computer Crime and Security Survey 2002*. AusCERT: Brisbane.

?? Taken from the Association of Superannuation Funds of Australia Ltd (ASFA) website at:
www.superannuation.asn.au.

?? Office of Strategic Crime Assessments, *The Future of Fraud in Australia*, [Assessment 8/98, November 1998].