Trends & issues
in crime and criminal justice

No. 470 July 2015

Australian Government
Australian Institute of Criminology

Misuse of information and communications technology within the public sector

Alice Hutchings and Penny Jorna

Misuse of information and communications technology (ICT) includes theft of hardware and software, unauthorised access to computer systems and inappropriate use of equipment. Internal unauthorised access is recognised as being a major contributor to data breaches, as employees may use legitimate access to computer systems in inappropriate and unauthorised ways. Risks of internal misuse of ICT in the public sector increase as new technologies emerge and more data about individuals are collated and stored by governments.

This paper examines how ICT has been misused in the past within Commonwealth entities. It draws on the findings of the Fraud against the Commonwealth cenuses collected by the Australian Institute of Criminology (AIC) for the 2008–09, 2009–10 and 2010–11 reporting periods to document the nature and extent of the problem.

Internal misuse of information and communications technology by public sector employees

ICT may be both the target of criminal activity, as well as a tool used to facilitate criminal acts (Choo, Smith & McCusker 2007). For the purpose of this paper, *internal misuse* refers to misuse by an employee or contractor of a government entity. By contrast, *external misuse* refers to incidents that are committed by individuals who are not an employee or contractor of the organisation. Instances of misuse of ICT within the public sector may fall within the definition of fraud provided in the Commonwealth Fraud Control Guidelines 2011 (the Guidelines), namely 'dishonestly obtaining a benefit, or causing a loss, by deception or other means' (AGD 2011: 5).

Foreword | *Information and communications technology (ICT) may be the target of criminal activity, as well as a tool used to facilitate criminal acts.*

Trust is placed in government employees to ensure that personal data are handled appropriately. However, there have been instances where this trust has been abused and data have been inappropriately accessed or otherwise used by insiders for illegitimate purposes. The misuse of ICT may also provide opportunities for financial gain, such as where accounting systems are manipulated by persons both within and external to agencies to commit fraud.

Using the findings from the Fraud against the Commonwealth cenuses collected by the Australian Institute of Criminology, data is presented regarding the misuse of ICT within the Australian Government over the three year period between 1 July 2008 and 30 June 2011. It is concluded that although the ICT environment is rapidly changing, fraud control plans, organisational policies and technical standards for data security minimise the risk of ICT misuse and identify intervention points at which prevention and detection methods may be focused.

Adam Tomison
Director

According to KPMG (2013), the most concerning frauds against organisations are those perpetrated by employees, as they tend to be committed for longer periods and may cause more reputational damage than external fraud. Over a three year period between 2008 and 2011, the estimated value of internal fraud against the Commonwealth has steadily increased, from $1.9m in 2008–09 (Lindley & Smith 2011) to $3m in 2010–11 (Jorna & Smith 2013). Internal misuse of ICT is an important area of concern as employees are often placed in a position of trust, which provides them with electronic access to personal information and records. Prior research has shown that in some instances, there are few checks on an employee's access (Smith & Jorna 2011). The outcomes of internal misuse can be damaging to the organisation and in the case of the public sector, taxpayers' confidence.

There are significant implications of misuse of ICT in the public sector, particularly owing to the amount of data that are held about individuals by governments. For example, data held by different tiers of government may include:

- health, income, employment and education information;
- details about contact with the criminal justice system;
- information such as address and date of birth; and
- photographs associated with licences and passports.

Data may also be collected that could track individuals' movements and daily activities, such as public transport usage. Misuse of ICT may also 'deplete government resources and have a negative impact on the administration of agencies', affecting the availability of funds for service and program delivery (Lindley, Jorna & Smith 2012: ix). Where misuse of ICT results in data breaches, there can be further negative impacts arising from the loss and subsequent misuse of individuals' personal information.

Relying on police and prosecution data to identify the extent of insider misuse of ICT does not provide a complete picture, as many matters go undetected, unreported, or may not have enough evidence or be serious enough to warrant investigation or prosecution (Lindley & Smith 2011). Not all misuse of ICT may be classified as criminal behaviour, but may instead violate the Australian Public Service Code of Conduct, organisational policies or attract civil remedies. Regardless of whether an incident involves the commission of a criminal offence, it may result in disciplinary action being taken, such as a formal warning, demotion or job loss.

Table 1 Agencies participating in the 2008–09, 2009–10 and 2010–11 surveys

	2008–09		2009–10		2010–11	
	n	%	n	%	n	%
Invited to participate	177	100.0	191	100.0	192	100.0
Responded	166	93.8	175	91.6	154	80.2
Included in analysis	149	84.2	152	79.6	154	80.2

Note: Percentages are of those invited to participate

Source: Commonwealth fraud surveys 2008–09, 2009–10 and Commonwealth fraud census 2010–11 data [AIC computer file]

Research questions

In order to understand misuse of ICT in the public sector, this paper addresses the following questions:

- What is the nature and extent of insider misuse of ICT in the public sector?
- What are the characteristics of those who engage in insider misuse of ICT in the public sector?
- What opportunities for ICT misuse are provided in the workplace?

Method

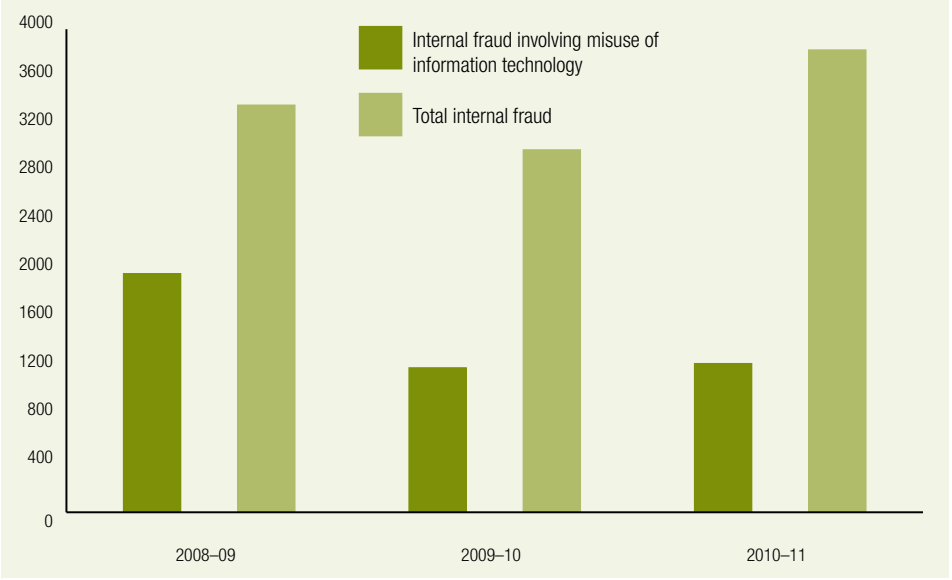
This research draws upon the results of the AIC's *Commonwealth Fraud Survey* for the 2008–09 and 2009–10 financial years and the *Commonwealth Fraud Census* 2010–11. The requirements for reporting on fraud and fraud control as set out by the Guidelines are outlined by Linley, Jorna and Smith (2012). Each year, the number of entities invited to participate differed slightly from the number that responded because new entities are created and others are removed or amalgamated. In addition, there are a small number of departments that choose not to participate for various reasons, including interests of national security. Finally, of the entities that did respond, some were excluded because they did not meet the eligibility criteria pursuant to the previous Guidelines. Entity particulars included in the analysis for each of the reporting periods are presented in Table 1.

Responding bodies completed a secure online questionnaire for each reporting period. The data collection examined two distinct categories of conduct—internal fraud and external fraud. The data included in the present analysis relates to internal frauds, defined as 'any incident of suspected fraud allegedly committed by an employee or contractor' (Jorna & Smith 2015: 11). The forms of misuse of ICT examined in this paper are:

- theft of telecommunications or computer equipment (including mobile devices);
- accessing information or programs via a computer without authorisation;
- copying or altering data or programs without authorisation;
- misuse of email;
- manipulation of a computerised accounting system;
- insertion of malicious code; and
- interference with computer networks.

Between the financial years, there were some slight variations in the wording of the questions asked in the questionnaire. However, the differences were not marked enough to prevent comparison between the results collected over the reporting periods. The 2010–11 census included an additional section relating to the most costly internal fraud incident experienced by each entity that had been concluded during the reporting period, irrespective of when the fraud had been committed. An incident was considered finalised once an

Figure 1 Total reported internal incidents of fraud and fraud involving misuse of ICT in 2008–09, 2009–10 and 2010–11 (n)



Source: Commonwealth fraud surveys 2008–09, 2009–10 and Commonwealth fraud census 2010–11 data [AIC computer file]

Table 2 Agencies reporting internal and external frauds involving misuse of ICT in 2008–09, 2009–10 and 2010–11

	Internal fraud		External fraud	
Reporting period	Agencies (n)	Agencies (%)	Agencies (n)	Agencies (%)
2008–09	23	15	10	7
2009–10	20	13	10	7
2010–11	24	16	13	8

Source: Commonwealth fraud surveys 2008–09, 2009–10 and Commonwealth fraud census 2010–11 data [AIC computer file]

Table 3 Theft of telecommunications or computer equipment (including mobile device) by reporting period (n)

Reporting period	Number of agencies	Total incidents
2008–09	16	70
2009–10	13	72
2010–11	10	45

Source: Commonwealth fraud surveys 2008–09, 2009–10 and Commonwealth fraud census 2010–11 data [AIC computer file]

investigation had been completed, referred to another body, or upon the suspect leaving the employment of the entity. Information was sought in relation to the suspect, or if the incident involved more than one person, the principal suspect.

To provide context to and illustrate the types of misuse of ICT that have been detected in the public sector, relevant case studies from the Commonwealth Director of Public Prosecutions' annual reports are also provided.

Nature and extent of misuse

Over the three years between 2008 and 2011, 4,403 incidents involving internal misuse of ICT were reported. As shown in Figure 1, 1,976 incidents were reported in 2008–09, however this decreased by 40 percent in 2009–10, down to 1,196 incidents. In 2010–11, there was a three percent increase, with 1,231 reported incidents. The proportion of total internal frauds that involve misuse of ICT has decreased in recent years, from 59 percent in 2008–09 to 32 percent in 2010–11.

Misuse of ICT was approximately twice as likely to be involved in internal, rather than external, frauds over the 2008–09 to 2010–11 periods (see Table 2). The following sections provide an overview of the internal fraud incidents involving ICT by type of misuse.

Theft of telecommunications or computer equipment (including mobile devices)

The value of computer equipment is greater than just the replacement cost of the hardware when the device(s) have been used to store proprietary or customer-related data. Computers and mobile devices may be targeted for this reason (Smith & Jorna 2011).

On average, 13 agencies reported having experienced theft of telecommunications or computer equipment each reporting period. The average number of incidents per year was 62 (of an average 3,400 internal fraud incidents per year). As shown in Table 3, there was a reduction in the number of reported thefts in the 2010-11 survey, down to 45 incidents from 72 the previous year.

Three agencies reported theft of telecommunications or computer equipment as being the most costly internal fraud incident concluded in 2010–11. One incident also involved accessing information via a computer without authorisation and therefore is discussed in the next section of this paper.

Of the two incidents covered here, both involved only one suspect. In addition to theft of telecommunications or computer equipment, both suspects had allegedly stolen other government equipment. The motivations for the thefts were unknown or not provided for either incident. The total financial losses caused to the agencies were $5,000 and $8,000. Losses were defined as 'the total amount, in whole dollars, thought to have been lost to the agency from fraud incidents, prior to the recovery of any funds, and excluding the costs of detection, investigation or prosecution'. One incident did not result in any financial recovery, while the other resulted in full recovery.

Table 4 Internal frauds involving misuse of ICT, by method, in 2008–09, 2009–10 and 2010–11 (n)

	2008–09		2009–10		2010–11		Overall total incidents
Type of fraud involving misuse of ICT	Agencies	Total incidents	Agencies	Total incidents	Agencies	Total incidents	
Accessing information or programs via a computer without authorisation	17	1,816	8	1,011	13	991	3,818
Copying or altering data or programs without authorisation	6	21	7	34	8	18	73
Misuse of email	3	9	8	35	9	57	101
Manipulation of a computerised accounting system[a]	2	3	4	4	-	-	7
Insertion of malicious code	0	0	0	0	0	0	0
Interference with computer networks	0	0	1	6	0	0	6
Unable to be determined	1	1	0	0	1	1	2
Other misuse of ICT	5	56	6	34	11	119	209

a: This response option was omitted from the 2010–11 survey

Source: Commonwealth fraud surveys 2008–09, 2009–10 and Commonwealth fraud census 2010–11 data [AIC computer file]

One of the incidents occurred over a period of six months, while the other occurred during a single month. Once detected, the incidents took between one and 13 months to be finalised. Both incidents were investigated by the agency, with one also being investigated by police. One suspect admitted to the allegation in full and had a legal sanction imposed. The other was dismissed from employment with legal proceedings incomplete at the time of the data collection period.

Accessing information or programs via a computer without authorisation

Data breaches can occur by accessing or copying data without authorisation. The number of compromised records may be one indication of the severity of the breach, as is the sensitivity of the data and how they are subsequently used. This is particularly relevant to the public sector, where employees and contractors can have access to sensitive information relating to individuals, government contracts, procurement details, business records and even national security issues.

Some context to accessing information without authorisation is provided by way of cases studies from the Commonwealth Director of Public Prosecutions. In 2007, a government employee resigned after being found to have accessed computer records over a two year period of people known or associated with people known to the individual. The matter proceeded to court, where the defendant pleaded guilty. The offences, motivated by curiosity, were found to have resulted from a 'mental condition' and the breakdown of a violent relationship (CDPP 2009). In another case, the alleged offender, a law enforcement officer, not only accessed data relating to a romantic interest and their partner, but also subsequently disclosed information relating to the latter to others (CDPP 2010).

In a case involving a consultant contracted to an Australian Government department, another's authentication credentials were used to access data after the offender's access was revoked. Over a period of 19 days, the offender accessed the records of 75 individuals. Convicted, the offender was originally sentenced to 12 months' imprisonment with a good behaviour condition of three years. The sentence was reduced to 50 hours of community service on appeal, primarily as the offender had not received any personal benefit (CDPP 2009).

Accessing information or programs using a computer without authorisation was the most commonly reported type of internal fraud, with 3,818 incidents reported over the three year period (see Table 4). However, the number of incidents reported had been declining, with the number almost halving from 1,816 in 2008–09 to 991 incidents in 2010–11.

Two agencies reported that the most costly internal fraud incident concluded in 2010–11 involved accessing information via a computer without authorisation. Each incident involved only one suspect, one of whom (as noted previously) had also allegedly stolen telecommunications or computer equipment, as well as other government equipment and misused ICT in other ways. While the motivation of one suspect was unknown, the other was reportedly motivated by greed and the desire for financial gain.

One incident occurred over a period of six months, while the other continued for seven years. Both incidents were investigated by the agency in question. One incident involved 'no further action' being taken, while the other was still under investigation at the time of the survey, with legal proceedings to be commenced.

For one incident, the total financial loss was $5,076, of which $2,688 (53%) was recovered from the suspect. For the other incident, the total financial loss was $524,789, of which $13,327 (3%) was recovered. This was the highest financial loss reported by participating entities in this section of the census.

Copying or altering data or programs without authorisation

Each year, Verizon, a company providing network, information system and mobile

Box 1 Copying or altering data or programs without authorisation

Over a three month period, the defendant, a Centrelink employee, created 26 Centrelink customer accounts in false names and caused benefits to be paid to those accounts. He then obtained the benefits paid.

The defendant also caused payments in the form of Electronic Benefit Transfers to be made to four accounts of Centrelink customers known to him without their authorisation. The defendant obtained the money for himself.

The defendant obtained a total amount of $66,120.36 and was charged with 30 counts of obtaining property by deception pursuant to s 134.1(1) of the Criminal Code. He pleaded not guilty at the committal hearing in the Magistrates Court of South Australia but subsequently pleaded guilty at his District Court trial.

The defendant was sentenced to a total sentence of four years imprisonment to be released after serving 18 months. In sentencing the defendant the Court stated:

> It is very serious offending involving gross breaches of trust on a sustained basis...I must bear in mind that the courts have made it clear on many occasions that in dealing with this sort of fraud, particularly where the person involved is a government employee, there is a significant need for the sentence to be such that it will deter others in a position of trust who are minded to attempt to defraud the welfare system.

Source: CDPP 2010: 19

technology products and services, publishes a report detailing data breaches that have been identified worldwide. In 2012, 14 percent of breaches involved those internal to the organisation. This is an increase from four percent in 2012, however, down from a high of 48 percent in 2009 (Verizon 2013).

In the *Commonwealth Fraud Survey 2008–09* and *2009–10* and the *Commonwealth Fraud Census 2010–11*, copying or altering data or programs without authorisation was reported 73 times over the three year period between 2008 and 2011. On average, seven agencies reported instances of unauthorised copying or altering of data or programs each financial year (see Table 4). None of the agencies reported copying or altering data or programs without authorisation as being the most costly internal fraud incident concluded in 2010–11.

Copying or altering data can lead to other offences. For example, in the case described in Box 1, altering data led to obtaining property by deception. In 2007, a similar matter was discovered that involved the creation of 65 false identities on the agency's database system that resulted in 387 fraudulent medical benefit claims to the value of $156,034.50 (CDPP 2010).

Misuse of email

Email misuse includes sending emails and attachments that contravene organisations' internal policies such as codes of ethics, email usage policies and sexual harassment policies. Some email misuse may also be considered illegal if it relates to the possession or distribution of child exploitation material or threatens, menaces, harasses or causes offence. Misuse of email can also contribute to other offences, such as unlawful disclosure (see Box 2).

In the *Commonwealth Fraud Survey 2008–09* and *2009–10* and the *Commonwealth Fraud Census 2010–11*, reported misuse of email increased almost fourfold from nine incidents in 2008–09 to 35 incidents in 2009–10. In 2010–11, the number of reported incidents increased another 63 percent to 57 (see Table 4). While this response option was omitted when asking about the most costly internal fraud incident experienced by each organisation, one entity did include misuse of email under the 'other' response category. As this incident also involved manipulation of a computerised accounting system, among other frauds, it is discussed in the following section.

Manipulation of a computerised accounting system

A variety of frauds can take place using computerised accounting systems, including redirecting funds to personal bank accounts, approving false invoices and creating 'ghost employees' for the purpose of receiving salary payments (Smith & Jorna 2011). In the *Commonwealth Fraud Survey 2008–09* and *2009–10* and the *Commonwealth Fraud Census 2010–11*, two entities reported that a total of three fraud incidents occurred as a result of manipulation of a computerised accounting system in 2008–09. This number increased to four entities each recording one incident in 2009–10. This response option was omitted in the 2010–11 questionnaire (see Table 4).

Two entities reported manipulation of a computerised accounting system as being the most costly internal fraud incident concluded in 2010–11. One incident involved only one suspect, while the other allegedly had seven other co-offenders.

In addition to manipulation of a computerised accounting system, one suspect was also suspected of theft of cash/currency (including theft of petty cash). The other was suspected of a number of additional frauds, including theft of consumable stock (office related), misuse of government equipment, misuse of agency courier accounts, misuse of email, accepting kickbacks and other corruption, namely 'abuse of power'. The motivation for one suspect was unknown, while the other was reportedly 'professional financial problems'.

One incident took place over a 45 month period, while the other occurred over 64 months. In both cases, the entities investigated the incidents and finalised the matters within four months. Outcomes of the investigations at the time of the census included one suspect admitting to the allegation in full with legal proceedings incomplete, while the other was referred to the Australian Federal Police with no legal proceedings undertaken. The total financial losses caused to the organisations were $15,638 and $129,960, with neither incident resulting in recovery of any of the funds.

Box 2 Misuse of email

The defendant was a senior public servant in the Indigenous Policy area of the Department of Families and Community Services and Indigenous Affairs. In that capacity, she forwarded an email outlining draft talking points for Australian Government diplomatic efforts in relation to the Draft Declaration of Rights for Indigenous People to her daughter. She also forwarded four emails on topics of dysfunction in outback Indigenous communities to a long-standing family friend… at a time when issues of Indigenous dysfunction were topical and the Australian Government was considering its response.

It was also alleged that the defendant had disclosed draft talking points for her superior's Senate testimony prior to the information being in the public domain and… she unlawfully disclosed to a long-standing family friend allegations of wrongdoing made against that family friend.

The defendant was charged with seven counts of unlawful disclosure by a Commonwealth officer pursuant to s 70(1) of the Crimes Act. On 28 August 2008, following a trial in the Supreme Court of the Australian Capital Territory, a jury found the defendant guilty of five counts. The defendant was acquitted on the count relating to the disclosure of her superior's Senate testimony and the jury were unable to reach a verdict on the count relating to the disclosure of allegation of wrongdoing made against a family friend. That count was later discontinued by the prosecution.

On 14 October 2008, in the Supreme Court of the Australian Capital Territory, the defendant was convicted and released on the condition that she be of good behaviour for three years and pay a pecuniary penalty of $2,000 within six months.

Source: CDPP 2009: 97

Insertion of malicious code

The potential outcomes of insertion of malicious code include account names and passwords being compromised, files being accessed or copied and corruption of hardware or software. Spyware, which can monitor computer activity, may be inserted intentionally by an employee to obtain sensitive information (Smith & Jorna 2011). Malicious code infections may result from other misuse, such as downloading and installing unauthorised software such as a game.

No incidents involving the insertion of malicious code by an insider were reported over the three year period (see Table 4). Similarly, there were no reports that insertion of malicious code had been the most costly internal fraud incident concluded in 2010–11. This is not to say that entities did not experience malicious code infections; rather, it may be hard to attribute infections to an individual or resulting from fraudulent intent.

Interference with computer networks

During the three years, only one organisation reported that an employee or contractor had interfered with computer networks; this was reported in the 2009–10 financial year. The entity advised that there had been six incidents involving interference (see Table 4). This entity reported that they had experienced six 'attempted denial of service' attacks. Denial of service attacks block access to online services, such as websites or accounts. This can occur by sending a flood of traffic to overwhelm websites to make them inaccessible to legitimate users.

None of the entities reported interference with computer networks as being the most costly internal fraud incident concluded in 2010–11.

Other types of misuse

Over the three years, 209 incidents involving other types of misuse of ICT were reported. In 2010–11, 11 agencies reported 119 incidents, an increase of 164 percent over the average of 45 incidents reported in the previous two periods (see Table 4). This increase was due to a report from one organisation of 102 instances of misuse of a point of sale system. Misuse of a point of sale system can conceal unauthorised transactions, as per the example provided in Box 3.

While five entities reported other misuse of ICT as being the most costly internal fraud incident concluded in 2010–11, two of these have already been discussed as they also involved misuse of ICT as covered in the preceding sections. Of the remaining three entities, each incident involved only one suspect.

One of the suspects was alleged to have used an 'inappropriate and extensive amount of email', as well as misuse of government equipment. Another was alleged to have used the 'departmental phone for personal purposes' as well as committing fraud in relation to travel expenses and expenses other than travel. The third suspect was alleged to have committed a number of frauds including:

- theft of other government equipment;
- theft of consumable stock (office related);
- misuse of government equipment;
- expenses other than travel, leave and related entitlements;
- theft of property other than cash; and
- false quotations for work.

In this case, it was reported that the alleged misuse of ICT was to 'circumvent procurement procedures' and prevent 'separation of duties'. The motivations of the three suspects were reportedly personal and family financial problems, psychiatric illness or mental disorder(s), and 'malicious and to cause trouble and mischief'.

The incidents occurred over a period of two months to two years, with an average of 12 months and three weeks. For the two incidents with a known detection date, the incidents had been finalised within eight and 15 months. All three incidents had been investigated by the entities. Outcomes of the investigations included one suspect being dismissed from employment with no

legal proceedings having been undertaken at the time of the survey. The other two suspects resigned or left employment, with one being dealt with under the entity's code of conduct.

One of the incidents did not cause the agency any financial loss. The financial loss caused in another incident 'could not be determined' and resulted in no recovery of losses. The third organisation reported a loss of $2,987, with the entire amount recovered from the suspect.

Characteristics of those who engage in internal misuse of ICT in the public sector

As well as detailing the nature of the offence, the most costly incident of fraud section included in the 2010–11 census asked about the suspects' demographic information. Of the nine suspects who were reported to have engaged in insider misuse of ICT in the public sector, seven were male, one was female and the gender of the remaining suspect was not disclosed by the organisation. Four of the nine suspects were aged 45 to 54 years. Two of the suspects were aged 55 to 64, two were aged 35 to 44 years and the remaining suspect was aged 25 to 34 years.

Eight of the nine suspects had been employed on a full-time basis, while the other was reported to have been employed overseas. All had been employed with the entity for more than four years. Five of the suspects did not hold a security clearance. Of the remaining four suspects, two held a clearance at the 'secret' level, one at the 'confidential' level and one at the 'protected' level.

While the highest education level for four of the suspects was not known, three had been educated to a graduate level and two to a postgraduate level. Five suspects had been employed at a middle management level, one at an intermediate level and one at an advanced level. The occupation levels for two suspects were not disclosed.

Box 3 Other types of misuse (point of sale system)

The defendant was the licensee of [a] Licensed Post Office. An audit of the Post Office conducted on 14 December 2007 revealed that $58,002.39 in cash was unaccounted for. The defendant told the auditors that he did not know where the money was. He subsequently declined to participate in a record of interview.

The Post Office kept cash in a safe. The defendant could not access the safe by himself as it had to be opened with two keys—one held by the defendant and one held by a security firm. It was later established that the defendant had been taking cash rather than depositing it in the safe and concealing the missing cash by making false accounting entries in the Electronic Point of Sale computer system. The accounts appeared to balance, however, the amount of money asserted to be held in the safe was incorrect.

On an evening prior to the security firm's monthly collection of the cash held in the safe, the defendant made an accounting entry that purported to withdraw cash from the safe, so that the amount of cash recorded as being in the safe matched the amount actually held. A security officer then collected the cash from the safe and recorded an amount matching the entry on the Post Office's accounts. After the collection, the defendant made an electronic entry reversing the withdrawal of the previous evening.

The defendant was charged one count of dishonestly causing a loss to a Commonwealth entity pursuant to s 135.1(5) of the Criminal Code.

On 6 July 2009, the defendant pleaded guilty in the Wollongong Local Court. On 27 October 2009, he unsuccessfully applied to reverse his plea. The defendant was sentenced to a total of 11 months imprisonment to be served by way of periodic detention and a reparation order in the amount of $58,002.39.

The defendant appealed against his conviction to the District Court of New South Wales. The appeal was dismissed on 19 March 2010.

Source: CDPP 2010: 15

Opportunities for misuse

The questions asked of respondents about the most costly internal fraud incident experienced provided a unique insight into the context surrounding those who were suspected of committing internal frauds. For instance, the finding that all of the incidents that involved misuse of ICT were allegedly committed by employees who had been with the entity for four or more years may be due to this extended time period enabling the offender to acquire knowledge about how the organisation operated and how to commit the alleged offence. In some instances, the offence had escaped detection for some time—up to seven years. The ability of an employee to evade detection for such a long period may be partly due to the individuals' knowledge of internal processes and control, whereby they can avoid routine security checks.

Where the occupational levels of the suspects were known, all but one had been in a middle management or an advanced level role. There are some different theories as to why those engaged in positions of greater responsibility may commit and/or be detected committing fraud. For example, those employed at higher occupational levels may be presented with more opportunities, may feel that their activities are less scrutinised, or they may have developed a misplaced sense of entitlement to the benefits received. An alternative explanation is that they may be no more likely to offend than those employed at lower occupation levels, however, they may be subject to greater

scrutiny and therefore their fraudulent activities may be more likely to be detected and subsequently reported. In addition, frauds conducted by those in higher positions may be of a higher value and therefore more likely to be captured in the most costly internal fraud incident section of the questionnnaire. Internal misuse of ICT was often not the sole offence the suspect was allegedly involved in. In one instance, misuse of ICT enabled other frauds by circumventing procurement procedures.

Of the 154 agency participants in the 2010–11 census, nine reported that the most costly internal fraud completed in 2011 involved some aspect of ICT. A further 35 entities reported that they had finalised a costly fraud matter in that reporting period that did not involve misuse of ICT. This section of the questionnaire also asked about how these incidents were detected. Respondents were permitted to select more than one response, which are detailed in Table 5. Interestingly, all but one of the incidents involving misuse of ICT was discovered during internal audits/investigations and/or by a staff member or colleague. The other incident was discovered by reportedly applying 'internal controls'. This indicates that internal oversight, whether formal by way of audits, or informal by way of confirming co-workers' suspicions, are useful in detecting misuse when compared with other methods. This was not dissimilar to frauds that did not involve misuse of ICT, where the most common ways frauds were discovered also involved internal oversight (Jorna & Smith 2015).

Discussion and conclusion

The ICT environment is rapidly changing and rates of, and opportunities for, misuse shift in reflection of this. The number of known internal fraud incidents involving the use of ICT has declined since 2008–09. However, internal misuse of ICT was reported by twice as many entities as misuse of ICT by those external to the organisation. The most commonly reported fraud type was accessing information or programs via a computer without authorisation, although the occurrence of this has reportedly declined to almost half the number of incidents recorded in 2010–11 when compared with 2008–09. Another explanation as to why the number of detected incidents may fluctuate is that organisations may change their practices in identifying misuse of ICT. For example, as emails are liable for collection under Freedom of Information requests, organisations may be more sensitive to misuse of, and more likely to monitor, these communications.

Most suspects who were alleged to have committed the most costly incidents reported by entities in 2010–11 were male, had been employed with the agency for many years and in all but one instance, were aged 35 years or over. While almost all offenders were believed to have operated alone, the one offender who reportedly colluded with others was suspected of working with seven co-offenders to commit frauds that included manipulation of a computerised accounting system. In this research, it was found that the majority of the suspected offenders held middle management (Executive Level 1 or 2) positions. The frauds were also committed over a sustained time period, on average for two years and three months, before detection.

All of the incidents were detected using internal controls. The most common penalty imposed was dismissal from employment, although legal proceedings had been imposed, or were expected to be commenced, in relation to a number of incidents.

It is noted that the 2010–11 queationnaire instrument collected further information about the most costly internal frauds. However, incidents that involve ICT, such as the loss of information, may not always incur a financial loss. Therefore, this may not capture those incidents that result in reputational damage and lasting effects to those external to the organisation.

While a reactive approach is important to identify and address misuse of ICT, it is likely that many instances of misuse of ICT go undetected and unreported. Fraud in general is known to be vastly underreported (Lindley, Jorna & Smith 2012) and fraud involving ICT may be particularly so. This may be due to policies not yet being in place that relate to evolving technology and the detection and prevention of misuse of ICT. Therefore, a proactive approach is important in preventing the losses and damage that can otherwise be incurred.

According to the Guidelines, all agencies are required to have fraud control plans that encompass prevention strategies, as well as policies on detection, reporting and investigation of fraud. Technical standards for data security, as well as organisational policies, also play a preventive role. Future AIC research will identify the prevention and control strategies that agencies can use to minimise risks of misuse of ICT, including the identification of intervention points at which prevention and detection methods might best be focused.

Dr Alice Hutchings is a Research Associate at the Computer Laboratory, University of Cambridge in the United Kingdom.

Penny Jorna is a Research Analyst at the Australian Institute of Criminology.

General editor, *Trends & issues in crime and criminal justice* series:
Dr Adam M Tomison, Director,
Australian Institute of Criminology

Note: *Trends & issues in crime and criminal justice* papers are peer reviewed

For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website at: aic.gov.au

ISSN 0817-8542 (Print)
1836-2206 (Online)

GPO Box 2944
Canberra ACT 2601, Australia
Tel: 02 6260 9200
Fax: 02 6260 9299

References

All URLs correct as at February 2015

Attorney-General's Department (AGD) 2011. *Commonwealth fraud control guidelines 2011*. Canberra: Attorney-General's Department. http://www.ag.gov.au/CrimeAndCorruption/FraudControl/Documents/commonwealthFraudControlGuidelinesMarch2011.pdf

Choo K-KR, Smith RG & McCusker R 2007. Future directions in technology enabled crime 2007–09. *Research and Public Policy series no. 78*. Canberra: Australian Institute of Criminology. http://aic.gov.au/publications/current%20series/rpp/61-80/rpp78.aspx

Commonwealth Director of Public Prosecutions (CDPP) 2010. *Annual report 2009–10*. Canberra: CDPP. http://www.cdpp.gov.au/Publications/AnnualReports/

Commonwealth Director of Public Prosecutions (CDPP) 2009. *Annual report 2008–09*. Canberra: CDPP. http://www.cdpp.gov.au/Publications/AnnualReports/

Jorna P & Smith RG 2015. Fraud against the Commonwealth: Report to Government 2010–11 to 2012–13. *Monitoring report 24.* Canberra: Australian Institute of Criminology

KPMG 2013. *A survey of fraud, bribery and corruption in Australia and New Zealand 2012*. Sydney: KPMG. http://www.kpmg.com/au/en/issuesandinsights/articlespublications/fraud-survey/pages/default.aspx

Lindley J, Jorna P & Smith RG 2012. Fraud against the Commonwealth 2009–10 annual report to government. *Monitoring report* no. 18. Canberra: Australian Institute of Criminology. http://aic.gov.au/publications/current%20series/mr/1-20/18.aspx

Lindley J & Smith RG 2011. Fraud against the Commonwealth 2008–09 annual report to government. *Monitoring report* no. 14. Canberra: Australian Institute of Criminology. http://aic.gov.au/publications/current%20series/mr/1-20/14.aspx

Smith RG & Jorna P 2011. Corrupt misuse of information and communication technologies, in Graycar A & Smith RG (eds), *Handbook of global research and practice in corruption*. Cheltenham: Edward Elgar Publishing Limited: 255–281

Verizon 2013. *2013 data breach investigations report*. http://www.verizonenterprise.com/DBIR/