Fighting fraud in the public sector III

41%

of government organisations globally experienced at least one instance of economic crime in the past 24 months (down from 46% in 2012)

34%

of these government organisations experienced more than 10 fraud incidents in the past 24 months

27%

of government organisations surveyed around the world suffered losses in the past 24 months that were in excess of US$1million

pwc


NO DANGEROUS GOODS IN TUNNEL
LOW TUNNEL CLEARANCE 4.4m
DETOUR

Introduction

Cassandra Michie

Partner,
Forensic Services

+61 (2) 8266 2774
cassandra.michie@au.pwc.com

The significant financial loss caused by fraud in the public sector continues to plague internal audit and risk teams. It is not just the one-off incident that we should be concerned about, but the increasing regularity of fraud – and changes in the origins of fraud. It is now time to take action to prevent, detect and fight fraud.

Welcome to *Fighting fraud in the public sector III*, which includes the results of PwC's Global Economic Crime Survey 2014.

The Global Economic Crime Survey has been conducted every two years since 1999 and in Australia since 2001. It is one of the largest and most comprehensive surveys of its kind.

For the latest report, we had our greatest global response rate to date: 5,148 respondents across 95 countries participated in the survey, with 279 respondents from the public sector.

Fighting fraud in the public sector III provides an overview of our survey with respect to the incidences of fraud and corruption in the public sector globally, as well as in the wider Australian economy. In addition to insights from various Australian state anti-corruption agencies, our analysis includes the number of instances and types of fraud that occurred.

The report also provides dedicated chapters on the high-risk areas of:

- procurement fraud
- cybercrime, including information and system security.

We have supplemented the findings of the Global Survey with a final section on the human resources problems that can create a workplace environment where fraud is more likely to occur.

PwC would like to thank all the Australian organisations that participated in the survey. We hope that this report will provide valuable insights and practical advice on how the public sector specifically can enhance its efforts to prevent, detect and fight fraud and other economic crime.

Cassandra Michie
Partner
Forensic Services

Contents

Snapshot

41%

of government organisations globally experienced **at least one instance** of economic crime in the **past 24 months**

(down from 46% in 2012)

34%

of these government organisations experienced more than **10 fraud incidents** in the **past 24 months**

27%

of government organisations surveyed around the world suffered losses in the past 24 months that were in excess of **US$1 million**

36%

of economic crime experienced by government organisations **was perpetrated externally**

(compared to 29% in 2012)

The Big 5

Asset misappropriation | **Procurement fraud** | **Bribery and corruption** | **Human resources fraud** | **Accounting fraud**

Key trends:
Emergence of the 'Big 5'

The vast majority of economic crime in Australia falls into the 'Big 5': asset misappropriation, procurement fraud, bribery and corruption, human resources fraud and accounting fraud.

Asset misappropriation remains the number-one economic crime for government, and for all industries in Australia and globally, accounting for 68 per cent of all economic crime in the public sector.

What we have seen in this year's survey is the clear emergence of **procurement fraud** as one of the most common forms of economic crime. Procurement fraud has more than doubled in the public sector since 2012, with 46 per cent of public sector organisations reporting this in 2014. This mirrored the findings of the anti-corruption commission reports from New South Wales (where 341 or 12 per cent of complaints related to 'improper use or acquisition of funds or resources') and Queensland (where 416 or 11 per cent of allegations related to 'misappropriation'). In this report we have dedicated a chapter to the procurement life cycle, our experience of the types of procurement fraud, and where the risks lie.

"Procurement fraud has more than doubled in the public sector since 2012."

The incidence of **bribery and corruption** has also risen in the public sector (from 24 per cent of organisations that experienced economic crime to 35 per cent). In Australia, bribery and corruption problems are large: annual reports from state anti-corruption commissions show that there were 238 allegations of bribery and corruption in New South Wales in the 2013 financial year, or an average of over four per week. In Queensland the figure was more than double this, averaging nearly 10 allegations per week.

Human resources fraud has also emerged as a risk for the public sector, with 32 per cent of organisations surveyed experiencing it. As the name suggests, human resources fraud is concentrated in the employee benefits function. It covers payroll fraud (including salaries, allowances and other benefits), nepotism in the recruitment process and the hiring of unqualified individuals.

In the previous edition of *Fighting fraud in the public sector*, we noted an increase in **accounting fraud** in the public sector, compared to a decrease in this type of crime in the private sector. This was attributed to the tightening of controls and investment in fraud prevention techniques in the private sector. It seems that public sector organisations have followed this lead, as incidents of accounting fraud have decreased from 32 per cent to 21 per cent of organisations since our last survey. This trend is encouraging, but more remains to be done to tackle this ever-present risk.

Although **cybercrime** has dropped out of the top five types of economic crime (accounting for only 16 per cent of organisations that experienced economic crime in the public sector), we are seeing it register in the corruption reports of the various state commissions. Western Australia recorded 350 allegations of misuse of computer systems (including email and internet) and 187 alleged breaches of confidentiality and misuse of information, while New South Wales recorded 543 allegations of improper use of records or information.

Incidents of fraud: *The types and costs of crime*

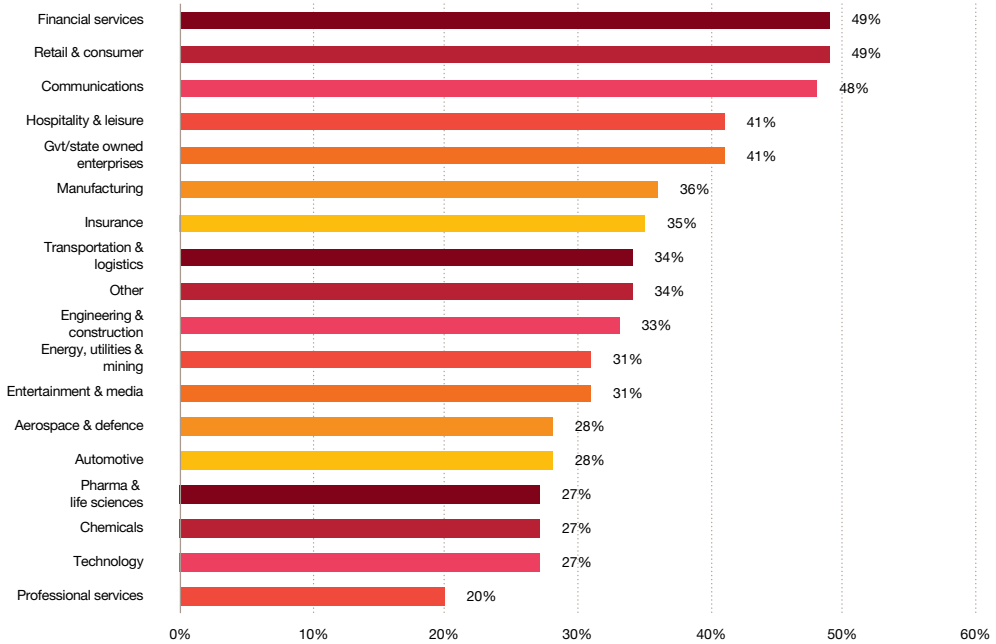
From our global survey, we saw a decrease in the number of frauds committed against the public purse: 41 per cent of representatives from the government and public sector reported experiencing one or more incidences of economic crime in the last 24 months, down from 46 per cent in 2012. This compares unfavourably to the 37 per cent of all organisations globally but favourably to the 57 per cent of all Australian organisations.

How the public sector compares

While the decrease in fraud instances for the public sector provides a degree of comfort, the public sector ranks equal fourth across all industries for instances of fraud. Only the financial services, retail and consumer, and communications industries experience a greater level of fraud.

Economic crime remains a very real risk for the government sector. Although prevention and detection strategies have matured, there is still room for improvement.

Economic crime by industry 2014



Our findings are consistent with the New South Wales Auditor-General's Report,[1] which had the following findings in the three-year period from 1 July 2009 to 30 June 2012.

State anti-corruption agencies

"The public sector ranks equal fourth across all industries for instances of fraud"

Our survey findings are also consistent with the reports of various state anti-corruption agencies, where the number of matters (not just corruption, but all matters reported) remains high. From 2011 to 2013, there was a substantial increase in the number of matters referred to anti-corruption commissions in Western Australia, and New South Wales remained relatively unchanged. In contrast, Queensland experienced a significant decrease, due to a reduction in complaints from health employees. This can be attributed to the establishment of 17 hospital and health networks in that state, where allegations appear to have been captured.

Number of matters (including corruption) referred to state anti-corruption commissions

	2011	2012	2013
NSW – Independent Commission against Corruption	2,867	2,978	2,930
VIC – Independent Broad-based Anti-Corruption Commission	n/a	n/a	667
WA – Corruption and Crime Commission	3,208	5,944	6,148
QLD – Crime and Misconduct Commission	5,124	5,303	3,949
SA – Independent Commission Against Corruption	n/a	n/a	n/a
TAS – Integrity Commission	190	108	66

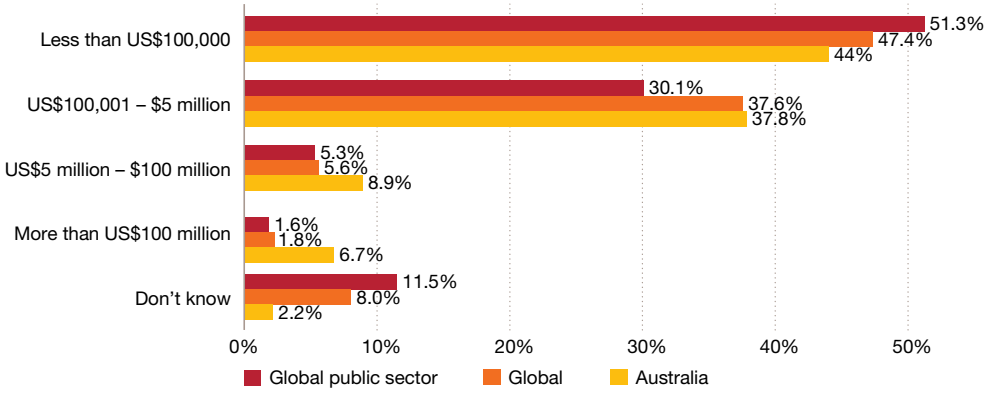
We note that the anti-corruption commissions in both Victoria and South Australia were recently created (2012), suggesting a (growing) need for such organisations. We await the first results for these two organisations with anticipation.

[1] Audit Office of NSW, 2012, '2012 Fraud Survey', NSW Auditor-General's Report to Parliament, vol. 7.

Counting the cost

Of those public sector organisations globally that experienced economic crime, just under half (49 per cent) reported a loss of greater than US$100,000.

Estimate of loss incurred by fraud

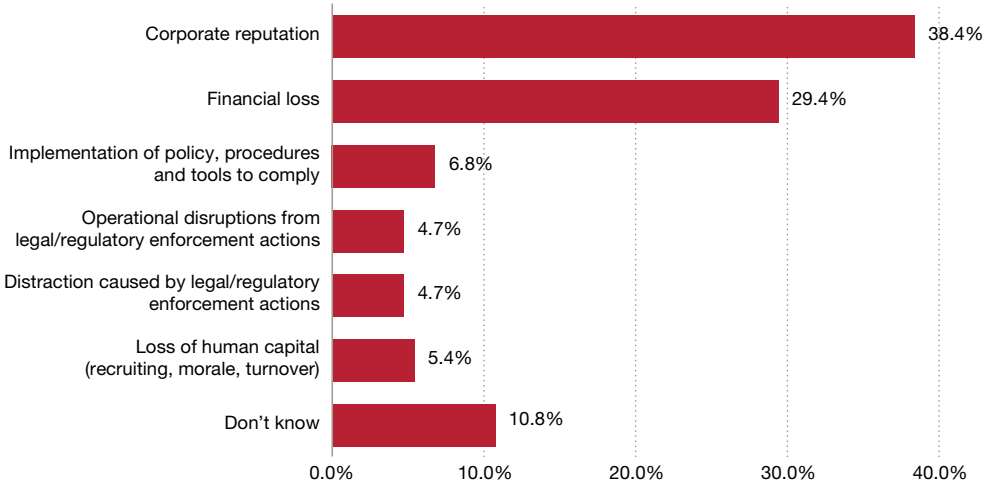


It should be noted that in addition to direct financial costs incurred as a result of an economic crime (including both the loss, and the costs to investigate and take remedial action), there are other commercial consequences, such as reputational/brand damage, deteriorated relationship with regulators, poor employee morale and service disruption.

In our experience, damage to a public sector agency's reputation rests heavily on public perception and has a long-term effect on the morale of employees.

"In addition to direct financial costs, there are other commercial consequences, such as reputational damage, poor employee morale and service disruption."

Most severe effect of corruption and bribery (public sector)

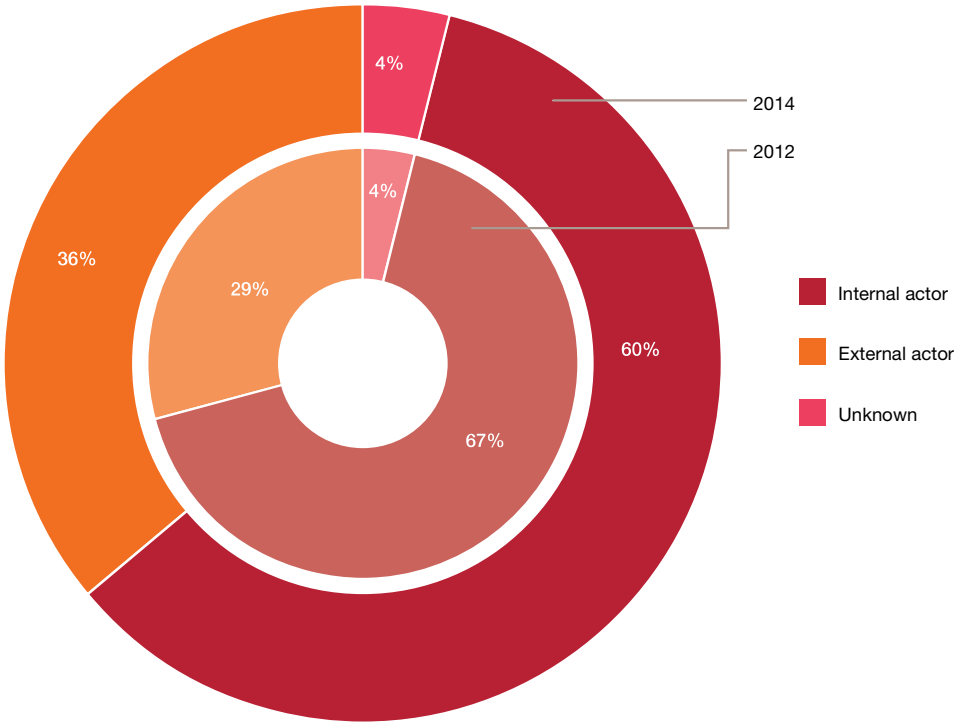


Identifying the perpetrators: *Profile of a fraudster*

For the public sector globally, most perpetrators of economic crime remain internal fraudsters (60 per cent). However, since 2012, the proportion of crime committed by external fraudsters has increased.

In Australia, the increase in external fraudsters has resulted in an almost even distribution between internal and external fraudsters (2014: 51 per cent external).

Profile of a fraudster



What does this mean for organisations? When fraud is occurring from all angles, it can be difficult to know where to focus preventative controls efforts. It is important to understand more about who these fraudsters are, and how their profile is changing.

CV of an internal fraudster in the public sector

Position:	Middle or senior management (74 per cent in 2014, up from 55 per cent in 2012).
Age:	41–50 years (43 per cent in 2014, up from 30 per cent in 2012). Public sector fraudsters are getting older. In our 2012 survey, the majority (35 per cent) were aged between 31 and 40.
Gender:	Male (66 per cent), although the number of female fraudsters is on the rise, increasing from 21 per cent in 2012 to 29 per cent in 2014 (4% did not specify gender).
Qualifications:	Qualified graduates (59 per cent in 2014, up from 47 per cent in 2012). Previously, most fraudsters held only high school qualifications. This shift may reflect the increasing education profile of the workforce generally.
Length of service:	Over 10 years (41 per cent in 2014, up from 26 per cent in 2012). Fraudsters today have been with the organisation longer.

Customers remain the main perpetrators of external fraud against public sector organisations (experienced by 33 per cent of organisations surveyed). Instances of fraud by vendors have halved since 2012 to 15 per cent, but frauds committed by agents or intermediaries have increased (20 per cent, up from 12 per cent in 2012). This might reflect the public sector's move to outsource various services, demonstrating the need for appropriate detection mechanisms and controls over dealings with outsourced providers.

Approaches to combating external fraudsters usually include a combination of preventative and reactive controls, such as due diligence over external relationships, so that the organisation understands who it is dealing with, followed by ongoing transactional analysis once a relationship is established.

By contrast, when dealing with internal fraudsters, organisations rely more heavily on reactive measures, often when it is too late: the fraudster may have long since left the organisation. When asked what factor they felt contributed the most to economic crime committed by internal fraudsters, Australian and public sector organisations globally overwhelmingly nominated opportunity or ability to commit the crime. This suggests that preventative measures are essential for combating these fraudsters. Later in this report we address in more detail preventative strategies to help reduce and deal with economic crime.

Who perpetrates economic crime is particularly relevant to this year's key theme of procurement fraud. In PwC's own experience with clients, most procurement fraud involves the external bribery of internal employees, in order to secure a contract, pay a fraudulent invoice or falsify expenses. Is this internal or external fraud? The reality is this type of fraud is collusive in nature. The most effective and lucrative procurement fraud schemes require an internal employee to be involved.

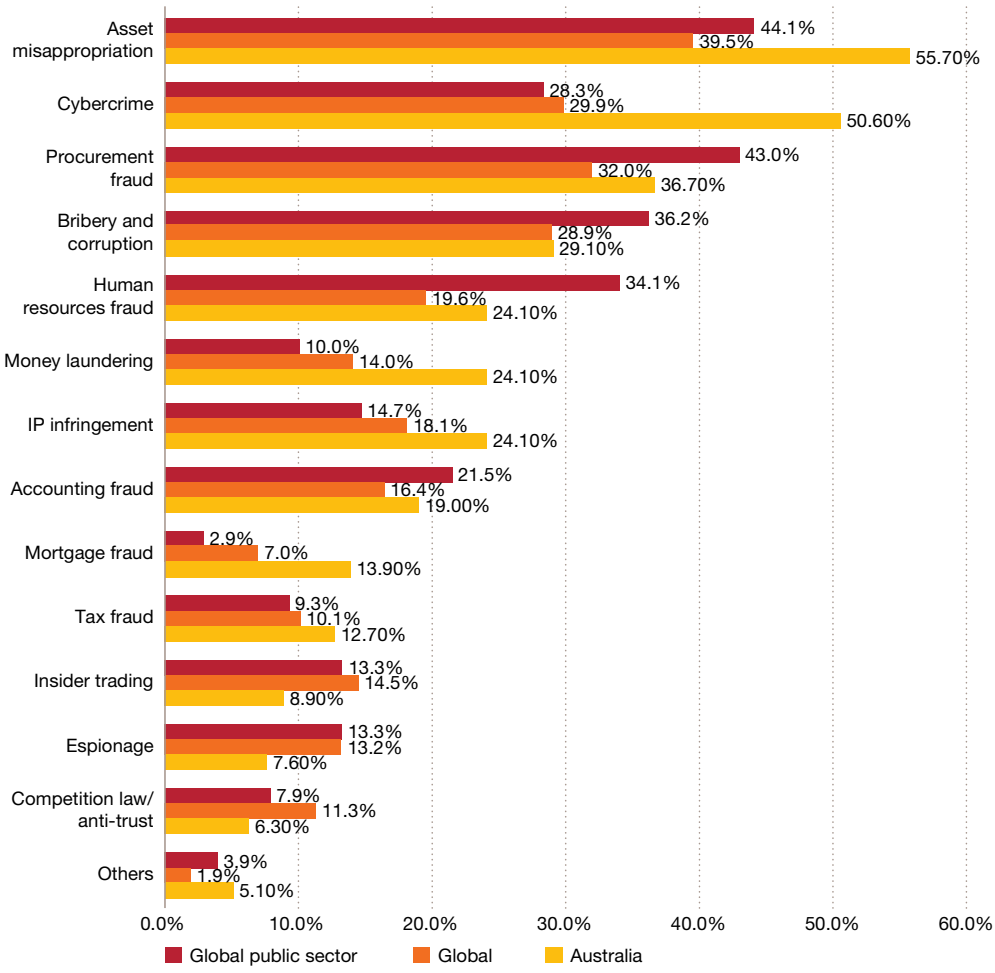
"In PwC's experience, most procurement fraud involves the external bribery of internal employees, in order to secure a contract, pay a fraudulent invoice or falsify expenses."

Looking to the future: *Where does the real threat lie?*

Australian organisations' perception of future risk of economic crime has increased. For the majority of economic crimes, Australian organisations rate the likelihood of experiencing economic crime more highly than their global counterparts do.

Public sector organisations perceive the greatest threat of future economic crime to have the same profile as the top three crimes already experienced: asset misappropriation, procurement fraud, and bribery and corruption. However, 34 per cent of public sector organisations also perceive human resources fraud as a significant future threat, more so than global and Australian organisations in general.

Perception of future crime



These high levels of perception of risk are not surprising, given the current levels of government and media interest in corporate governance issues generally, and more specifically fraudulent behaviour. The question of risk is now well understood at senior levels of most organisations, and by boards in particular, who are mindful of the damage to reputation that poor governance or inadequate fraud management can cause. Perceptions of future risk are clearly important when considering the management and mitigation of those risks.

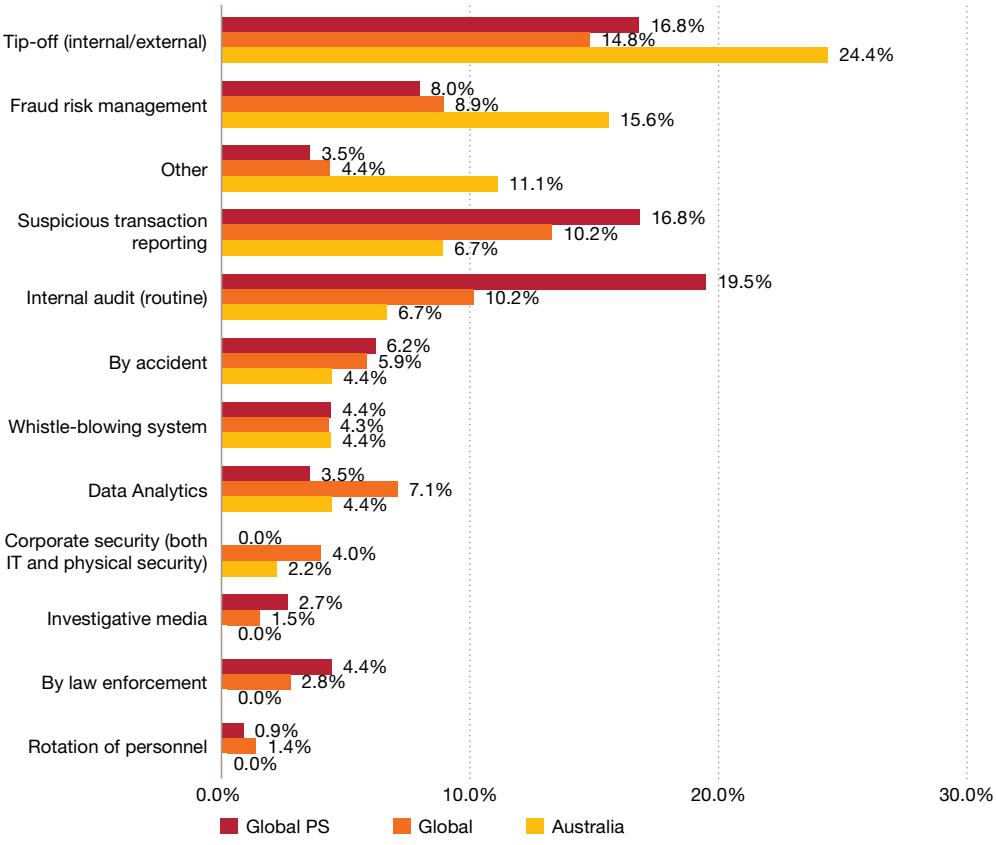
It is also interesting to note the differences in risk perception. Cybercrime registers at just over 50 per cent of perceived future economic crime for Australian respondents generally, whereas public sector respondents globally consider the risks of cybercrime to be just under 30 per cent. This perception gap could represent a blind spot for governments, with departments at greater risk than they perceive. Later in this report we discuss some Australian government agencies' specific experiences of cybercrime, and the types of risk that they may encounter.

"34% of public sector organisations perceive human resources fraud as a significant threat."

Detection and response: *What happens once corruption occurs?*

As always, it could be suggested that an increase in the reporting of experiences of economic crime in any organisation or industry could be as a result of improved detection methods.

Fraud detection



According to our survey, economic crime in public sector organisations globally is most usually detected as a result of routine internal audits, followed by tip-offs and then by suspicious transaction analysis. Reflecting the findings of our last survey, it would appear that the global public sector continues to lag behind Australian and global organisations in general in its use of formal fraud risk management tools. We found that nearly 40 per cent of public sector organisations did not know whether they had performed a fraud risk assessment in the last 24 months.

It is interesting to note that one-quarter of global public sector organisations stated the reason they had not performed a fraud risk assessment in that time was a perceived lack of value, while approximately 15 per cent of Australian organisations noted fraud risk management as the method by which economic crime in their organisation had been detected, second only to internal and external tip-offs.

Surprisingly, data analytics is still languishing below 10 per cent as a method of detecting fraud. In our experience, data analytics is a powerful tool for identifying high-risk or suspicious transactions. What is often lacking is the time commitment to sort through the false positives and follow up on unusual transactions.

There is strong data demonstrating that data analytics is effective. For example, the Australian Department of Veterans' Affairs recently saved $22.7 million by identifying improper benefit payments through its data matching program.[2]

On the improve

Our experience is that many Australian public sector organisations have significantly improved, or are trying to significantly improve, their performance in fraud detection and response. The New South Wales Auditor-General reported that two-thirds of agencies considered their fraud risk assessment to be highly effective.[3] The Commonwealth Fraud Control Guidelines specify that Commonwealth agencies must undertake a fraud risk assessment (internal and external risks) at least once every two years. We recommend state regulators consider issuing more holistic fraud control frameworks and guidelines, similar to the Commonwealth's.

We also believe that the tip-off numbers in our survey are understated for the Australian public sector, as suggested by the number of complaints received by the various state corruption commissions.

"Nearly 40 per cent of public sector organisations did not know whether they had performed a fraud risk assessment in the last 24 months."

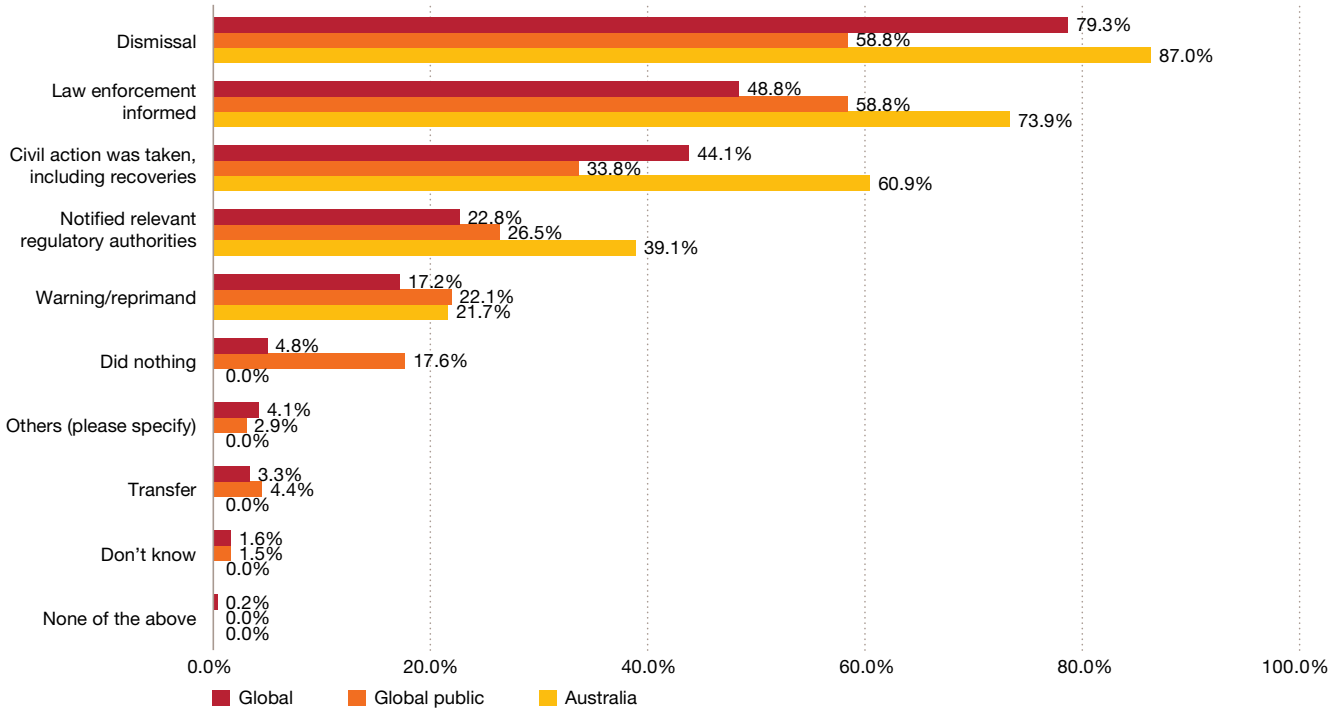
[2] ANAO, 2014, 'Fraud Control Arrangements', ANAO Report No. 3 2014–15.
[3] Audit Office of NSW, 2012, '2012 Fraud Survey', NSW Auditor-General's Report to Parliament, vol. 7, pp. 44.

"Public sector organisations took stronger action against external than internal perpetrators."

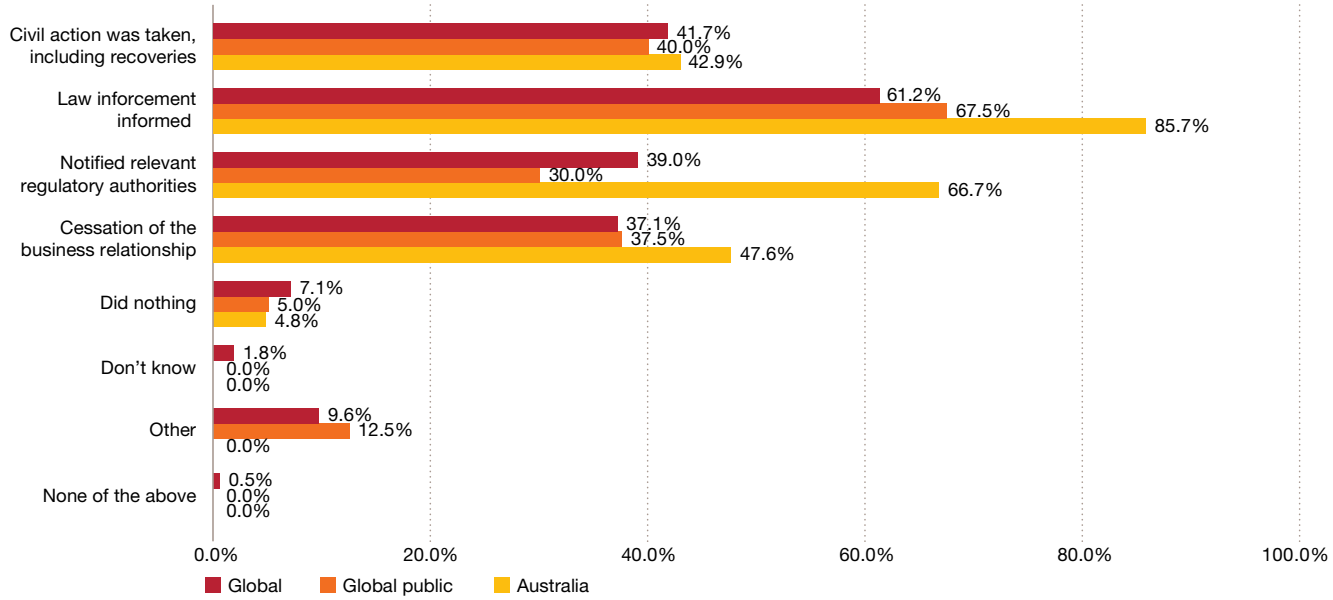
Responding to internal and external fraud

In all comparable forms of response to economic crime, public sector organisations responding to our survey took stronger action against external than internal perpetrators. Indeed, 18 per cent of organisations took no action against internal perpetrators, compared to 5 per cent for external perpetrators. This appears to be an incongruous response when the greatest threat of economic crime committed in the public sector comes from inside organisations.

Response to internal perpetrator



Response to external perpetrator



Procurement fraud: *On the take is on the rise*

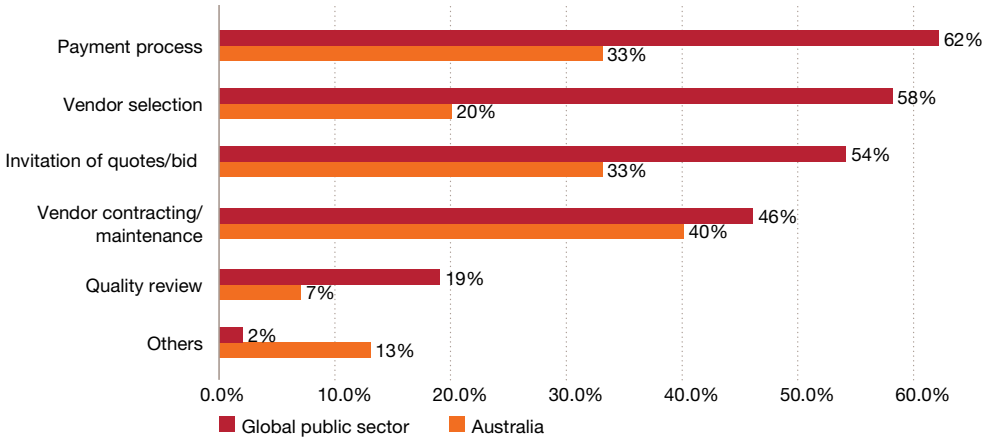
Globally, procurement fraud is now one of the 'Big 5' economic crimes, with 33 per cent of Australian respondents experiencing this type of fraud in the past 24 months. This rises to 46 per cent for global government organisations surveyed.

The procurement life cycle is a hotspot for fraudsters, because it is one of the primary areas of expenditure for government organisations. The procurement fraud life cycle may be illustrated as follows:

The procurement fraud life cycle

Procurement fraud is often complex to investigate because it can occur at any stage of the procurement life cycle. Globally, fraud occurred most often during the payments process stage, followed closely by the vendor selection and invitation of quotes/bids stages. Overall, for Australian respondents, vendor contracting and maintenance was the stage at which most procurement fraud occurred. But for the government sector, the payments process was the most common point of attack, followed closely by vendor vetting and selection.

Where did procurement fraud occur?



Globally, alongside government/state-owned enterprises (46 per cent), the industries reporting the most procurement fraud included energy, utilities and mining (43 per cent), engineering and construction (42 per cent) and transportation and logistics (39 per cent). Interestingly, these are all sectors where significant elements of their operations depend on close collaboration with governments, government entities and prime contractors likely to follow tendering processes.

How procurement fraud occurs

- Failure to follow organisation's procurement policy and guidelines in awarding contracts to suppliers (eg bypassing thresholds by awarding contracts without a market tender process).
- Inappropriate or poor contracting, including inappropriate terms and conditions favourable to the supplier.
- Collusion by an employee with an external vendor to defraud the employer (eg inflated contract prices, approving invoices for incomplete or substandard work). Employees may receive kick-backs, bribes or other incentives, or even be involved with the vendor in some capacity (eg as a consultant, director or shareholder).
- Establishment of a 'ghost' supplier or shell company to defraud through contracts, invoices and other payments.
- Contract variations and increases to contract value made after contract commencement, and without market testing.
- Inappropriate charges under cost-plus contracts, including cost/labour mischarging, defective parts and product substitution.
- Falsification of documents, including fraudulent invoices.

Strategies to consider

In our experience, most incidents of procurement fraud can be prevented or detected early, if the organisation possesses a complete understanding of:

- the procurement framework (policies and procedures)
- the risks involved in the procurement life cycle
- how controls and review mechanisms will actually reduce risks.

"The payment process was the most common point of attack in the procurement life cycle."

Consider whether the following components of your procurement framework are in place across the procurement life cycle:

Invitation of quotes and bids process/Vendor vetting and selection

- Procurement decision making is centralised and standardised or there is centralised management and supervision of procurement decisions.
- The procurement policy reflects the scale and risk of procurement, for example how to make a decision to go to tender, the number of quotes required for each purchase or whether a sole provider is appropriate.
- The procurement process is clearly mapped to identify the key controls and risks in the process.
- The tender and selection policy is communicated to all relevant staff.
- There are review mechanisms to ensure that approved vendors are used and government procurement rules are followed.
- Evaluation criteria are confirmed *before* starting the tender process.
- The evaluation criteria allow a like-for-like comparison.
- An independent panel assesses the tenders: the project manager may advise the panel but should not vote on the decision.
- Staff involved in procurement and who have procurement and payment delegations have appropriate and regular training on procurement policies and procedures.
- Vendor due diligence is conducted for major suppliers, including financial (credit position, financial capacity, insurance) and qualitative considerations (reputation, associated entities).

- Vendors must provide declarations of ethical conduct and/or compliance with code of conduct guidelines.
- An independent officer, in consultation with the project manager, is involved in any direct negotiations with the vendor.
- There are controls in place to ensure that the value of the proposed contract is not split or reduced to circumvent any thresholds regarding going to tender.

Vendor contracting and maintenance

- Order prices are compared to tender documents, vendor contracts, purchase orders or agreed price lists. This comparison covers both material pricing and hourly pricing.
- Contract variations as to delivery, service and pricing are reviewed and the need to retender is considered.
- Approved vendors are established and goods can only be ordered from these suppliers.
- The duties of individuals ordering goods and those receipting goods are clearly segregated.
- There is an established process for emergency procurement, and any purchases made through this channel are reviewed by senior management to ensure that minimal purchases are made in this manner and adequate records have been maintained.

Quality review

- Training is conducted regularly to ensure staff are aware of procurement fraud risks and the red flags to look out for. This may be a combination of code of conduct training for all staff and tailored procurement fraud training for procurement staff.
- A gifts and entertainment register is maintained to monitor potential supplier influence.
- Annual conflict of interest declarations, particularly for procurement staff, are required under the company's code of conduct.
- Staff are required to declare secondary employment.
- Managers conduct random monitoring.
- Reviews and testing of procurement are included in the internal audit plan.
- Problems relating to quality are documented and followed through with heightened monitoring: often quality issues are only discussed informally and let go until randomly identified in the future.

Payments process

- Delegations of authority are established and monitored for compliance.
- Invoices are matched to authorised purchase orders.
- Proof of delivery has been confirmed.
- Vendor invoices are reviewed against internal supporting documentation for correct:
  - labour – hours (against timesheets or contract estimates), skills and costs (including margins, allowances and per diems)
  - materials – costs (on-costs and GST), delivery (confirming receipt), quality (inspection of goods to meet contact specifications)
  - overhead – calculations (as per vendor contracts).

Procurement is by far the greatest fraud risk in the public sector. We encourage government entities to actively review and challenge their processes and controls, undertake risk assessment, and review and update their detection mechanisms.

"Government entities should actively review and challenge their processes and controls, undertake risk assessment, and review and update their detection mechanisms."

Cybercrime:
The need to be vigilant

Information security is an emerging issue for government: our survey found that 16 per cent of economic crime experienced by public sector organisations was cybercrime. The various state anti-corruption commissions also report a high number of allegations relating to information security. For instance, in Western Australia there were 350 allegations of misuse of computer systems (including email and internet) and 187 allegations of breach of confidence and misuse of information. New South Wales reported 543 allegations of improper use of records of information, while in Queensland there were 291 allegations in relation to control of information.

Characteristics of cybercrime

Recent reports by US-based cybersecurity firm Mandiant show that:[4]

100%

Percentage of recent major breaches involve the use of valid credentials (eg insiders or compromised insider credentials)

229

Average number of days from compromise to detection

2/3

2/3 of detections came from external sources, that is, the compromised organisation did not detect the event(s)

40

Average number of systems are touched/involved as part of a significant breach

The key message here? Organisations have a long way to go before their defences can be considered optimal. Also, the traditional security model of hardening the perimeter, focusing on only selected components, and inward-looking tactics are insufficient.

Based on recent media reports, the type of information most at risk includes:

- **Market-sensitive information:** an Australia Bureau of Statistics employee allegedly passed on market-sensitive information to a National Australia Bank employee, who then allegedly used this knowledge to profit from trades in foreign exchange derivatives.[5]
- **Customer records:** a number of Centrelink employees are alleged to have been searching customer records of family members and acquaintances and, in some instances, making changes to records that enabled higher benefits to be paid.[6]
- **Tender information:** an employee of the Western Australian Department of Planning allegedly downloaded submitted tenders and passed this information on to a rival business, where they were subsequently employed.[7]
- **Personal data:** the identities of four tax agents were allegedly stolen from the Australian Taxation Office and used to fraudulently obtain AUSkeys, giving access to specialist tax agent online services (the tax agent portal).[8]

[4] Merza M, 2014, 'Operationalizing advanced threat defense', and Goldberg J, 'Good guys vs bad guys – using data to counteract advanced threats', papers presented at *Splunk.Conf2014*, Las Vegas, August 2014.
[5] 'Two men arrested for insider trading and abuse of public office, $7 million restrained', 2004, Australian Federal Police media release, 9 May 2014.
[6] Dearne K, 2011, 'Centerlink cracks down on misconduct', The Australian, 14 December 2011.
[7] 'Former public servant to face court over unlawfully downloading confidential information', Australian Broadcasting Corporation News, 22 July 2013.
[8] Grubb B, 2013, 'Criminals breach Australian tax system', The Sydney Morning Herald, 9 February 2013.

In relation to cybercrime, public sector organisations appear to fare better than Australian organisations in general. Our survey confirmed the increasing impact of cybercrime on business, with 33 per cent of Australian respondents reporting that they experienced cybercrime in the last 24 months, and one in 10 Australian organisations reporting financial losses of over $1 million. However, the question of who in the organisation is accountable for responding to the threat of cybercrime needs to be addressed. Recent cyber-breaches have seen senior executives standing down as well as chief information officers. There is increasing awareness of cyber-threats among management and boards.

Cybercrime registers at just over 50 per cent of perceived future economic crime for Australian respondents, whereas public sector respondents consider the risks of cybercrime to be just under 30 per cent. This perception gap could represent a blind spot for government, leaving departments at greater risk than they realise.

Reinforcing this, 64 per cent of Australian CEOs in the 2014 PwC Australian CEO Survey said they were concerned about cyber-threats and a lack of data security. That being said, businesses continue to treat cyber-threats as an information technology problem, when in reality it is a whole-of-business problem. Good security requires a focus on the most important data; given the huge amount of data that is now produced, safeguarding everything is not possible. Some information will be more valuable than others, and identifying and classifying the most valuable 'trophy' data will allow organisations to prioritise security to protect this information.

"Cybercrime is having an increasing impact on business, with 33 per cent of Australian respondents reported experiencing cybercrime in the last 24 months"

Strategies to consider

- Identify what information is important, sensitive or valuable, such as awarding of contracts, market-sensitive information, issuing of new policies, or decisions to which access needs to be protected.
- Assess the quality of the controls protecting that information. A key area of risk is information that would allow identity fraud.
- Have clear policies about what constitutes confidential information and what are employees' responsibilities with respect to that information, covering:
  - protection of information
  - inappropriateness of accessing information not relevant to an employee's responsibilities
  - restrictions against sharing confidential information with other parties.
- Have detection systems in place, such as regular reviews of system-access logs, to identify where employees are inappropriately accessing information. A good tip is to identify access out of usual business hours (when fewer people are around and employees are more likely to access records inappropriately).
- Have a tight policy on user access and password controls (including password changes) to ensure secure access is available only to the appropriate people.

"In an electronic age organisations must be vigilant and keep pace with emerging threats."

Cybercrime often involves a faceless perpetrator. This can make it harder to identify threats. But today we live in an electronic age and organisations must be vigilant and keep pace with emerging threats. We encourage government entities to review their perception of the risk and to consider the security of those assets and information and data that are of greatest value and that are most susceptible.

Supplement: *Creating workplaces that discourage fraud*

PwC's experience has shown that an environment with high levels of workplace disputes and problems can harbour higher incidences of staff misconduct such as theft and fraud, as well as assault, intoxication or violation of contract and of code of conduct. In recent years, we have seen an increase in the incidence of behavioural and workplace misconduct allegations, particularly in relation to bullying and harassment.

Conflict and grievances are natural, inevitable, and part of the dynamics of any workplace. But environments with high levels of grievance take a significant toll on individuals, and diminish productivity through distraction, absenteeism and, in more serious cases, stress leave and insurance claims. At their worst, such environments can lead to loss of life, where there is a strong correlation between sustained stress and depression.

Grievances can arise in response to a number of factors, such as:

- performance management, including productivity pressure from metrics and budgets
- management decisions, team structure and rostering
- organisational restructure or change
- work environment and workplace safety.

Stress claims brought by employees

- The number of 'accepted' mental stress claims[9] in Australia (for 2008–09 to 2010–11 combined) was 21,400.[10]
- The number of 'accepted' mental stress claims in Australia for 2010–11 was 10,385, compared to total 'accepted' claims of 301,980.[11]
- In Victoria, stress claims represented 8 per cent of all total workers' compensation claims during 2001–02. This compared with 3.6 per cent prior to 1992–93.[12]
- In New South Wales during 2002–03, stress-related claims represented over one-third of all major claims for occupational disease.[13]
- Stress is the second-most common cause of workplace compensation claims in Australia, after manual handling.[14]
- Figures show that while compensation claims made by Australian employees fell significantly between 1996 and 2004, the number of stress-related claims almost doubled.[15]
- More workers are making psychological stress-related compensation claims than ever before, with the national cost of such claims estimated to be $105.5 million in 2000–01.[16]

9. Reports consider only claims that were accepted, not the total number of claims made.
10. Safe Work Australia, 2013, 'The Incidence of Accepted Workers' Compensation Claims for Mental Stress in Australia', April 2013, p. 19, www.safeworkaustralia.gov.au/sites/SWA/about/Publications/Documents/769/The-Incidence-Accepted-WC-Claims-Mental-Stress-Australia.pdf.
11. Safe Work Australia, 2014, 'Psychosocial Health and Safety and Bullying in Australian Workplaces', first edition, p. 2, www.safeworkaustralia.gov.au/sites/swa/about/publications/pages/psychosocial-health-and-safety-and-bullying-in-australian-workplaces.
12. Workcover Victims Victoria, 2009, 'Stress claims produce mixed legal messages', 3 October 2009, http://workcovervictims.blogspot.com.au/2009/10/stress-claims-produce-mixed-legal.html.
13. Workcover Victims Victoria, 2009, 'Stress claims produce mixed legal messages', 3 October 2009, http://workcovervictims.blogspot.com.au/2009/10/stress-claims-produce-mixed-legal.html.
14. Victorian WorkCover Authority, 2014, 'Stress', www.vwa.vic.gov.au/safety-and-prevention/health-and-safety-topics/stress.
15. Australian Safety & Compensation Council, 2008, cited in 'The cost of workplace stress in Australia', August 2008, Medibank Private, www.medibank.com.au/Client/Documents/Pdfs/The-Cost-of-Workplace-Stress.pdf.
16. Australian Psychological Society, 2004, 'Workplace stress: environmental and individual factors', October 2004, www.psychology.org.au/publications/inpsych/stress/.

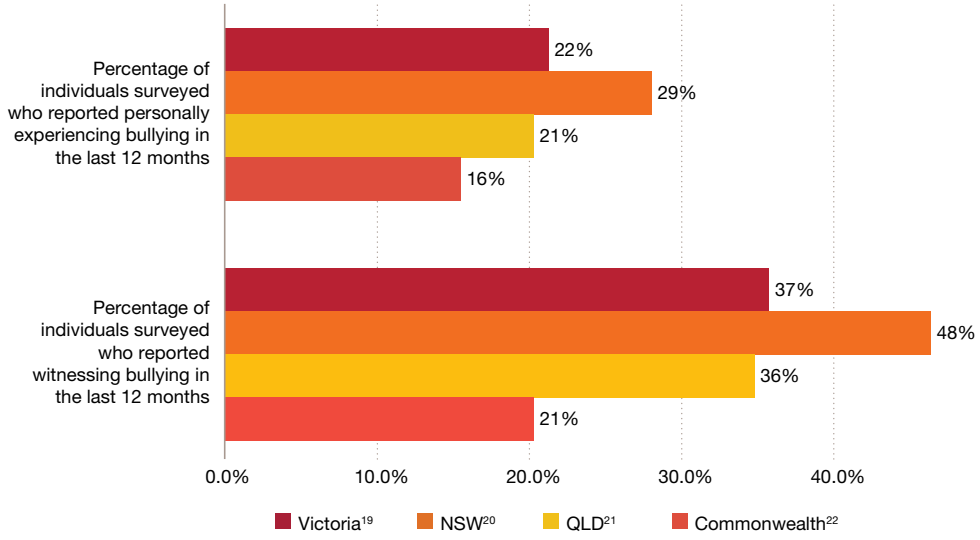
Surveys on workplace bullying

Current legislation requires all private and public sector organisations to protect the health, safety and welfare of people at work from behaviour that amounts to bullying or harassment. However, surveys of public sector employees indicate that bullying is common in government agencies.[17]

Statistics from the Queensland corruption agency state that victimisation/harassment and sexual misconduct together accounted for 12 per cent of all complaints about public sector employees in financial year 2013 (up from 10 per cent in the prior year). In Western Australia, assault, unprofessional conduct (demeanour/attitude/language), inappropriate behaviour and bullying/intimidation/harassment accounted for 26 per cent of all complaints of allegations received by that state's Corruption and Crime Commission.[18] Comparable statistics were not available for the New South Wales Independent Commission Against Corruption, although 27 per cent of reported allegations related to human resource and staff administration.

Results of public sector people surveys conducted by the various state-based bodies indicate that experiencing and witnessing bullying in the workplace is a common occurrence.

Workplace bullying in Australia



In the Fair Work Commission's first quarterly report after the introduction of the amendments mentioned below, it reported receiving 151 applications from workers for an order to stop bullying at work. Of the applications that specified the size of their employer (123), around half (54 per cent) came from businesses with 100 or more employees. The applications came from a wide range of industries, those with the highest number of applications being clerical (15 per cent) and retail (9 per cent).The majority of applications (69 per cent) alleged unreasonable behaviour by the complainant's manager. Of the finalised matters (56), eight were finalised by a decision and only one order was made in relation to actions that were required by the employer and applicant/complainant.

17. State Services Authority, 2010, 'Tackling bullying', Victoria.
18. The other state-based agencies did not stratify their complaint allegations in the same way, so we were not able to identify complaint types across all states.
19. Victorian Public Sector Commission, 'The state of the public sector in Victoria 2012-2013', p. 135, www.ssa.vic.gov.au/products/view-products/the-state-of-the-public-sector-in-victoria.html.
20. NSW Public Service Commission, People matter employee survey 2012: main findings report, p. 24, www.psc.nsw.gov.au/About-the-Public-Sector/People-Matter-Employee-Survey/People-Matter-Survey-2012.
21. Queensland Public Service Commission, Working for Queensland employee opinion survey 2012-2013, p. 56, www.psc.qld.gov.au/publications/workforce-statistics/assets/2013-WFQEOS-Final-Report.pdf.
22. Australian Public Service Commission, Sate of the service 2012–2013, p. 67, www.apsc.gov.au/__data/assets/pdf_file/0018/29223/SOSR-2012_13-final-tagged2.pdf.

Preventing and detecting workplace problems

A number of studies in the late 2000s and early 2010s, including the Standing Enquiry into Workplace Bullying (*Workplace bullying: we just want it to stop*) led to changes to the *Fair Work Act 2009* (Cth), effective 1 January 2014. These legislative amendments apply to some public sector organisations (exclusions apply for local and state government) but, importantly for all organisations, they provide a national definition for bullying, and clarify that reasonable management action carried out in a reasonable manner is *not* bullying.

A focus on improving culture over time will reduce the risk of such workplace problems arising. The following preventative and detective processes and programs will avoid workplace misconduct and disputes in an organisation.

Transformation

Policy, procedure and processes

- Review relevant policies, procedures and training materials to ensure compliance with relevant legislation.
- Review and assess effectiveness of policies and processes related to workplace behaviours.

Improvement

- Undertake workplace cultural 'health checks', for example via eSurveys.
- Undertake 'culture interviews' of selected managers and staff.
- Improve communication about changes and enhance staff development programs to improve communication skills.
- Assess the gap between what is expected and the resources available, then make bona fide changes to close the gap.
- Use investigation outcomes and recommendations to improve organisational policies and processes and culture across the organisation.

Investigating workplace matters

A number of workplace initiatives can contribute to a stronger workplace culture, which in turn will help to lower the risk of bullying, fraud, and other economic crime.

1. Investigative response

Independent investigation of specific grievances or allegations of misconduct can identify hotspots or areas of concern. This information can then be used to improve culture and processes/controls to reduce the risk of recurring misconduct. A variety of evidence is relevant when investigating workplace grievances:

Verbal evidence

- Informal or formal fact-finding interviews
- Formal investigative interviews
- Walkthroughs or sharing understanding of systems and control weaknesses

Electronic evidence

- Focused review of email correspondence (by period or specific search criteria such as keywords or correspondence between specific individuals)
- Analysis of electronic data relevant to the allegation, for example financial data, employee access data or computer login data

Documentary evidence

Review of relevant hard copy documentary evidence such as shift or timesheet data

2. Grievance mediation or facilitation process

Mediation

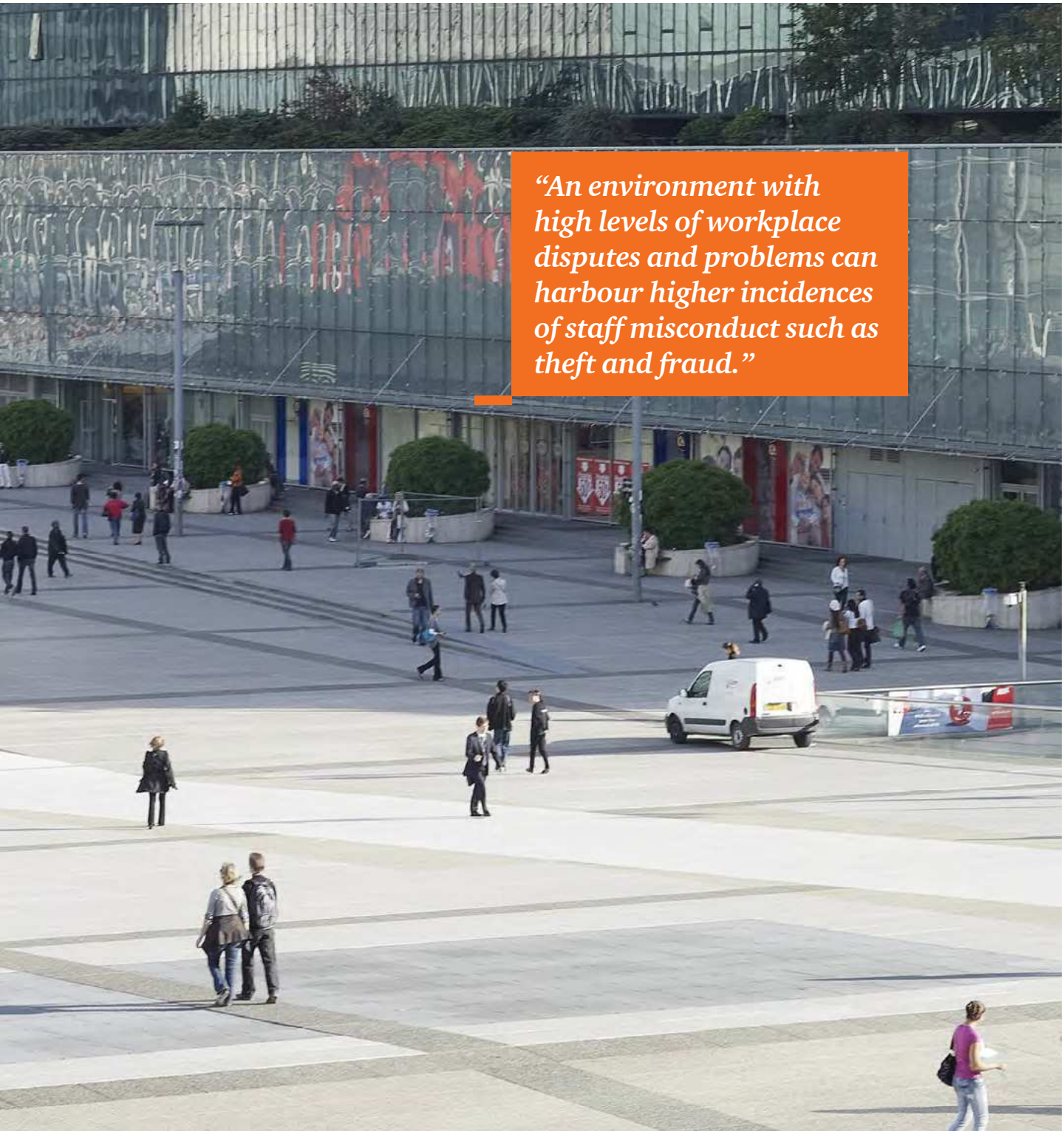
Mediation is a problem-solving process used to resolve grievances, disputes and conflicts. A mediator does not take sides or determine who is right or who is wrong. Rather, mediation:

- is an informal, yet structured, process to lead and prompt the resolution of grievances and disputes, guided by mediators acting as impartial third parties.
- helps individuals to hold honest discussions, to feel safe in expressing emotions, and to work through problems in order to reach a resolution.

Facilitation

- Facilitated discussions to assist parties in making decisions regarding future interactions and processes, including the development of ground rules.

PwC considers that workplace culture is a significant influence on the level of fraud in a workplace. The fraud control framework can be useful to reduce risks and harm in this area.



Conclusion: *Where to from here?*

Through the establishment of government anti-corruption agencies and their heightened profile and activity, there appears to be greater awareness of the risk of economic crime in the public sector. But it remains a very real threat, with 41 per cent of public sector organisations across the globe experiencing economic crime in the past two years.

The rising incidences of procurement fraud means the threat needs to be constantly evaluated, as procurement approaches evolve and move to more specialised or tailored models.

The emerging risk of workplace misconduct also needs attention, as it can lead to greater incentive to hurt or retaliate against an organisation by perpetrating fraud.

We would also challenge the public sector to reconsider its perceptions of cybercrime risk and to fully understand its susceptibility and the vulnerability of important information.

Reputation continues to be of paramount concern to public sector organisations. The loss of respect caused by negative headlines, the administrative burden and collateral damage that an incident of economic crime brings cannot be underestimated. It is vital therefore that organisations invest in fraud prevention and detection methods and that senior management and audit committees set the right tone by demonstrating, encouraging and rewarding ethical behaviour.

"Economic crime remains a very real threat, with 41% of public sector organisations experiencing economic crime in the past two years."

Procurement fraud

- For government organisations, the payment process is the most vulnerable to corruption, followed by vendor vetting and selection.
- Procurement fraud can usually be prevented or detected early if the organisation has a complete understanding of the procurement framework and life cycle.
- Combating external fraudsters requires a combination of preventative and reactive controls (eg due diligence over external relationships, followed by ongoing transactional analysis once a relationship is established).

Human resources workplace misconduct

- Organisations must set clear policies and training on workplace behaviour.
- A rapid response is needed, to deal with problems as they arise, rather than allowing situations to escalate.
- Managers must be aware of all the ways in which aggrieved staff can retaliate, such as through non-compliance with policies, or economic crime.

Cybercrime

- Cybercrime is a whole-of-business issue, involving not just technology but people and processes.
- Organisations must identify which information is important, sensitive or valuable, and needs to be protected against unauthorised access.
- Detection systems are needed to identify where employees are inappropriately accessing information.
- A tight policy on user access and password controls ensures that access is available only to the appropriate users.

About the survey

The 2014 Global Economic Crime Survey was completed by 5,128 respondents from 95 countries, with 279 respondents from the public sector.

Further information on the survey demographics and definitions of economic crime can be found in the Global Economic Crime publication online at www.pwc.com/crimesurvey.

pwc.com.au

For more information please contact:

Cassandra Michie
Partner, Sydney
+61 (2) 8266 2774
cassandra.michie@au.pwc.com

Tony Peake
National Leader – Government and Education
+61 (3) 8603 6248
tony.peake@au.pwc.com

Anya Gielen
Senior Manager, Melbourne
+61 (3) 8603 3803
anya.gielen@au.pwc.com

Kim Cheater
Partner, Adelaide
+61 (8) 8218 7407
kim.cheater@au.pwc.com

Craig Fenton
Parter, Brisbane
+61 (7) 3257 8851
craig.fenton@au.pwc.com

Natalie Faulkner
Director, Perth
+61 (8) 9238 3331
natalie.faulkner@au.pwc.com

127021807