# Corruption: From the backroom to the boardroom

**57%**

*of surveyed Australian organisations experienced economic crime in the past 24 months.*

**47%**

*of surveyed Australian organisations experienced in excess of 10 fraud incidents in the past 24 months.*

**36%**

*of surveyed Australian organisations suffered losses in excess of AUD 1 million in the past 24 months.*

pwc

# Introduction


**Malcolm Shackell**

**Partner,**
**Forensic Services**

+61 (2) 8266 2993
malcolm.shackell@au.pwc.com


I am pleased to present the Australian results of PwC's Global Economic Crime Survey 2014.

The Global Economic Crime Survey is one of the largest and most comprehensive surveys of its kind. The global and Australian surveys are conducted every two years, with the last release in 2012.

The latest survey results show that economic crime persists globally and is on the rise in many economies. As highlighted in our last survey, the world is aware of the risks of cybercrime yet both the Australian and global results suggest there are a number of often overlooked economic crimes that are occurring with increasing volume, frequency and sophistication. These crimes include procurement fraud, bribery and corruption, and human resource related fraud.

In Australia, procurement fraud and bribery has been increasingly prevalent most notably in the construction, mining and utilities industries.

The Australian supplement to our Global Economic Crime Survey will explore these and other issues in greater detail.

We would like to thank all the Australian participants in the 2014 survey. We hope the information within this report will provide valuable insight and practical advice on how organisations can continue their efforts to combat fraud and other economic crimes.

**Malcolm Shackell**
Partner

# Contents

# Snapshot

**57%**
*of Australian organisations experienced crime in the* ***past 24 months***
*compared to 47% in 2012*

**47%**
*of Australian organisations experienced in excess of* ***10 fraud incidents*** *in the past 24 months*

**36%**
***suffered losses*** *in the* ***past 24 months*** *that were in* ***excess of $1 million***
*compared to 16% in 2012*

## *The profile of reported perpetrators has changed.*

*Of internal fraudsters ...*

**65%** *are now from* ***middle management*** *(up from 45% in 2012) and*

**30%** *are* ***tertiary qualified*** *(up from 10% from 2012)*

## *Organisations experiencing* ***economic crime***

**57%**
*of Australian respondents ...*

**32%**
*of organisations in the Asia Pacific region ...*

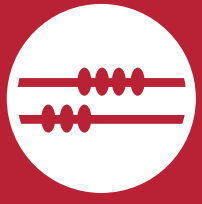
**37%**
*of organisations globally ...*

## *The Big 5*

***Asset misappropriation***

***Cybercrime***

***Procurement fraud***



***Accounting fraud***

***Bribery and corruption***

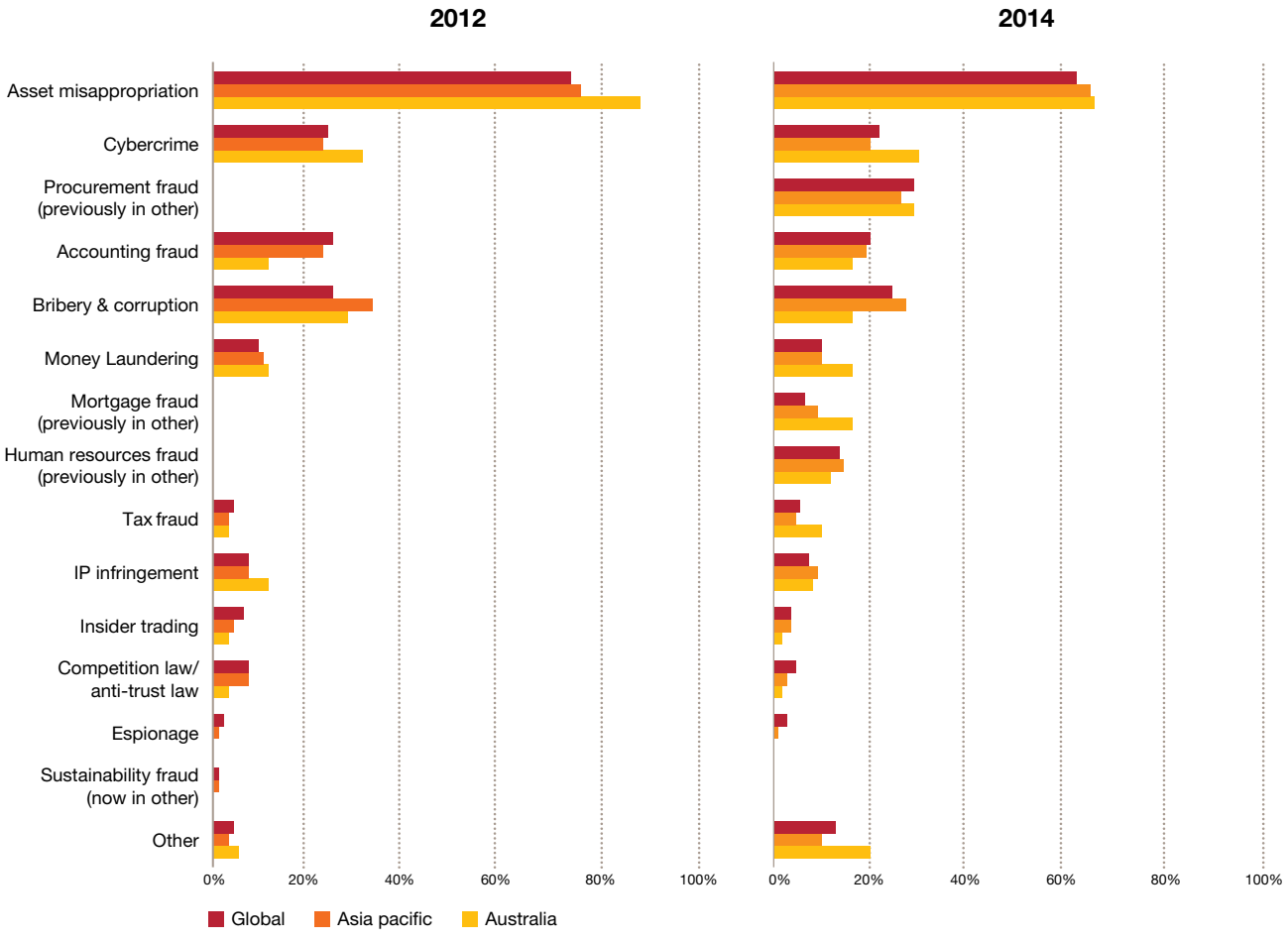
# The emergence of the 'Big 5'

*Asset misappropriation remains the number one economic crime experienced globally, in the Asia pacific region and in Australia. Australian organisations report higher rates of economic crime than experienced globally in the areas of asset misappropriation, cybercrime, procurement fraud, money laundering, tax fraud and IP infringement.*

Globally, and within Australia, the top three economic crimes are asset misappropriation, cybercrime and procurement fraud. In previous surveys, Australia's experience with procurement fraud was not expressly measured (it was included in the 'other' type of fraud), however we have expressly surveyed it in 2014 and the results are surprising. Procurement fraud has become the second most economic crime experienced by Australian organisations, and globally it is number three. Cybercrime has continued to rise in Australia too, up to 33 per cent from 30 per cent in 2012.

We are now beginning to see the emergence of the '**Big 5**' economic crimes; with procurement fraud and cybercrime firmly in the top three. Asset misappropriation, accounting fraud and bribery complete the Big 5.

**Economic crime rates: 2012 vs 2014**



# Australia: How do we compare?

Continuing the trend from 2012, in the past 24 months Australian organisations have reported significantly higher rates of economic crime than the average rates within the Asia Pacific region and globally.

In 2014, 57 per cent of Australian respondents reported that they had experienced economic crime. This is a jump of 10 per cent since 2012. By comparison 32 per cent of organisations in the Asia Pacific region and 37 per cent of organisations globally reported experiencing economic crime in the same time frame.

This does not necessarily mean that there is more economic crime in Australia, it may be indicative of more effective detection. Certainly, our statistics suggest that Australian organisations are applying effective detective controls such as data analytics and whistleblowing services more commonly than in many other economies.

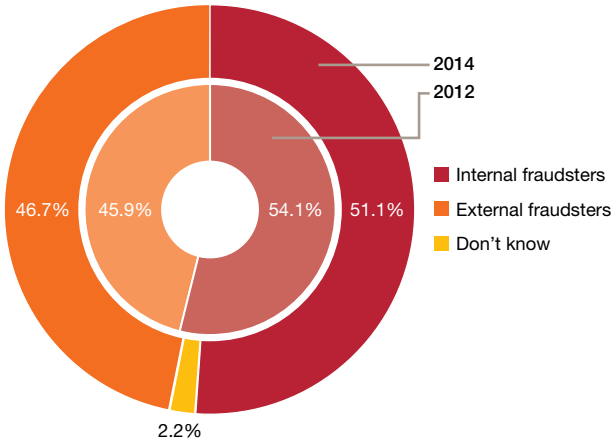
One other reason for the increasing higher rates of economic crime in Australia is that during times of economic stress, the components of the fraud triangle (rationalisation, incentive and opportunity) are intensified. Regardless of reported rates of occurrence, economic crime remains a threat to business processes, and may be considered a more strategic threat once particular types of economic crime are considered (such as a major cybercrime incident or systemic fraud leading to business collapse or regulatory sanction).

It is also possible that our mining, energy and construction sectors - which typically employ contract services, labour and equipment - have experienced high levels of fraud particularly in the procurement cycle. This is a trend we have observed in our day to day interactions with organisations operating in these sectors.

*Reporting of economic crime in Australia continues to increase and is higher than the global average.*

# *Profile of a fraudster*

**Thinking about the most serious crime in the past 24 months, who was the main perpetrator? 2012 vs 2014**




The primary perpetrators of economic crime remain internal fraudsters. However since 2012 the proportion of crime committed by external fraudsters has increased resulting in an almost even distribution between internal and external fraudsters.

What does this mean for organisations? It can be difficult to know where to focus preventative controls efforts when fraud is occurring from all avenues. It is important to understand more about who these fraudsters are:

- Internal fraudsters are:
  - increasingly **middle management** staff (65 per cent in 2014 up from 45 per cent in 2012)
  - primarily between the ages of **31-40 years** (52 per cent in 2014 and 55 per cent in 2012)
  - primarily **male** (57 per cent), however the number of female fraudsters is rapidly on the rise increasing from 25 per cent in 2012 to 39 per cent in 2014
  - increasingly **qualified graduates** (30 per cent in 2014 up from 10 per cent in 2012). Previously fraudsters primarily held **high school qualifications**. This shift may reflect the increasing education profile of the workforce.
- External fraudsters – increasingly are **customers** (48 per cent in 2014 up from 36 per cent in 2012).

Approaches to combating external fraudsters are usually a combination of preventative and reactive controls. For example the 'real time' credit card fraud detection suites that a number of retail banking organisations have implemented.

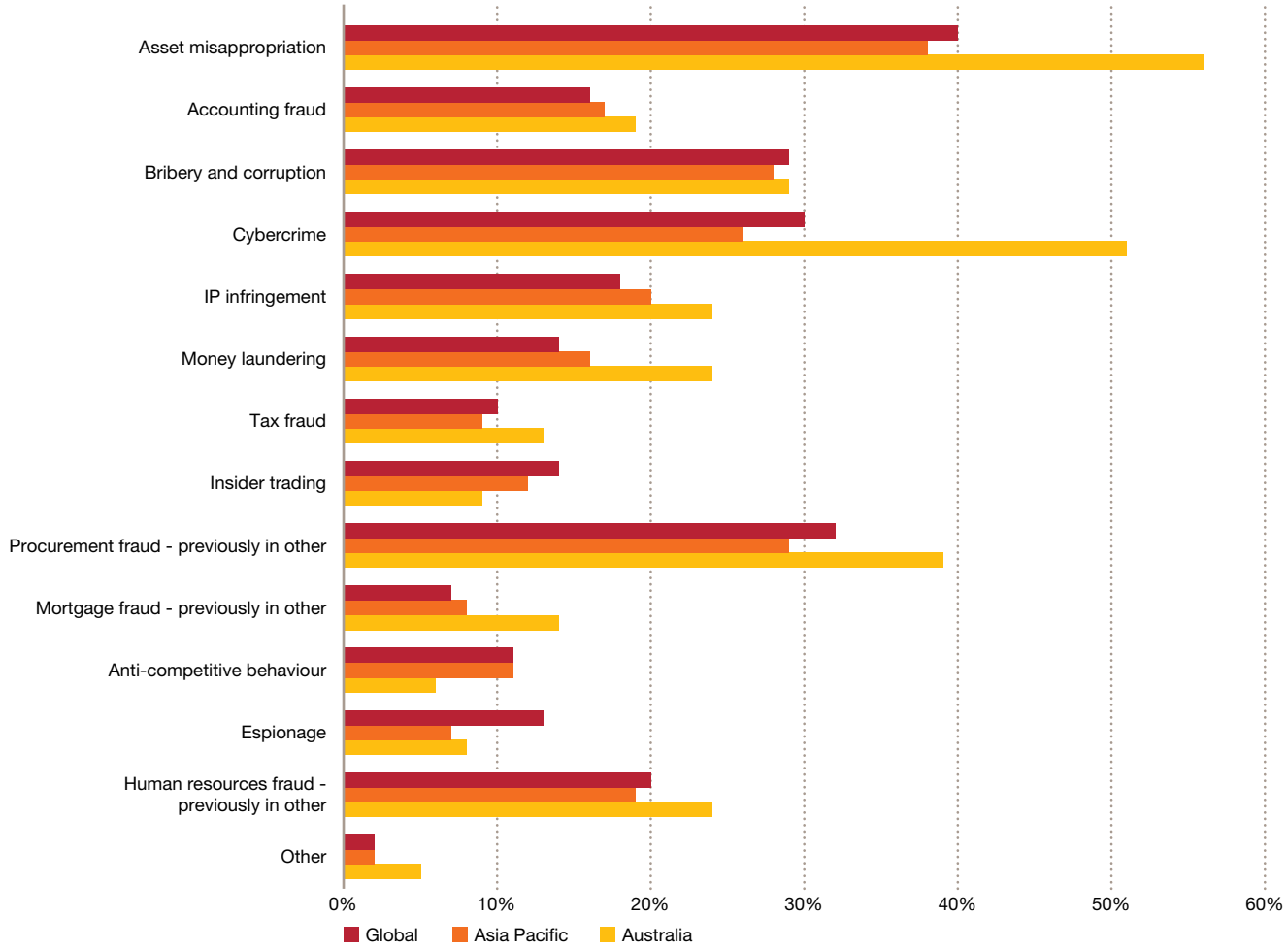
By contrast, when dealing with internal fraudsters, organisations rely more heavily on reactive measures, often when it is too late to deal effectively with the fraudster who may have long since moved on from the organisation. When asked what factor they felt contributed the most to economic crime committed by internal fraudsters, organisations overwhelmingly (74 per cent) felt it was due to opportunity or ability to commit the crime. This indicates that a focus on preventative measures is a key approach to combating these fraudsters.

Who perpetrates economic crime is particularly relevant to this years' key theme of procurement fraud. In our experience most procurement fraud is facilitated through 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.

# *Perception of future crime*

The perception of risk of economic crime to Australian organisations in the future has increased. For the majority of economic crimes, Australian organisations rate the likelihood of experiencing economic crime higher than their global counterparts.

**Perception of future crime**




Perceptions of future risk are clearly important when considering the management and mitigation of those risks.

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 focus on risk is now well understood at senior levels within most organisations and by Boards in particular, who are mindful of reputation risks that poor governance or inadequate fraud management can create.

# *Detecting fraud*

The Australian survey results suggest that in general, Australian organisations are very good at detecting fraud, and are also more proactive around implementing techniques to identify potentially fraudulent schemes and transactions.

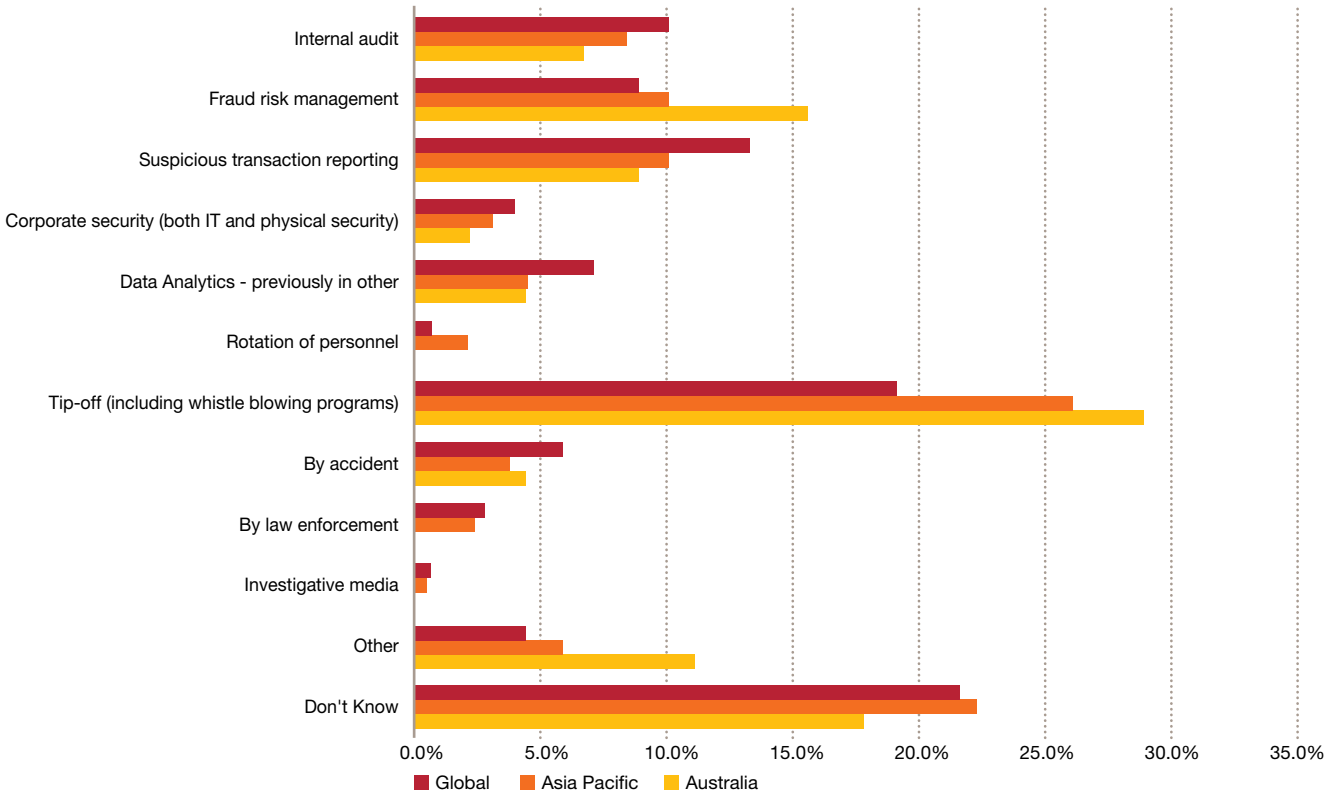
Close to a third of Australian organisations (29 per cent) are detecting economic crime through tip-offs from internal and external sources and formalised whistleblower programs. Australian organisations take the time to consider fraud risk management and are thus able to pinpoint the areas of fraud risk in their organisations, and prepare accordingly.

In this way, fraud management and detection techniques can be applied more efficiently and with more focus. For example:

- utilising specific fraud profiling analytics over high risk business processes such as accounts payable and contracting
- placing more scrutiny over certain types of expenditure such as credit cards, entertainment, donations and travel
- focussing internal audit reviews on issues such as asset write downs and stock disposals, both areas of increasing fraud risk in many organisations.

As the results show, there is a welcome trend in the proportion of Australian organisations implementing formal whistleblower programs. Equally as important, we have noticed that many are implementing protocols around training, awareness, management and investigation of whistleblower complaints. Whistleblower programs are only as effective as the management of the complaints.

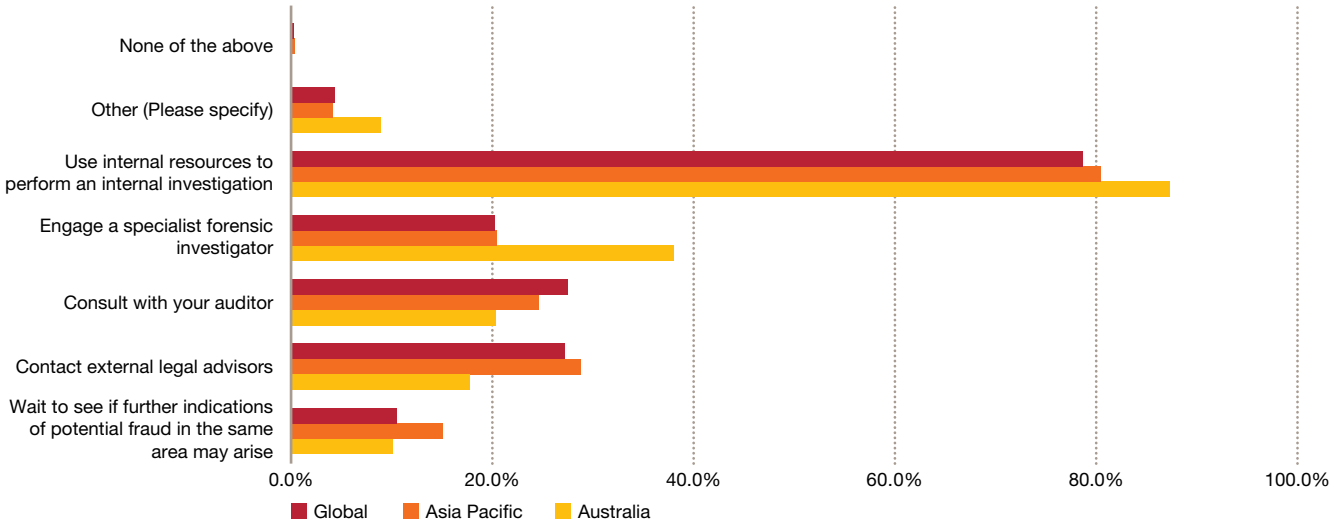
**Thinking about the most serious economic crime experienced, how was the crime initially detected?**



The survey results also show that Australia is ahead of its global peers in regard to the investigation of suspected fraud incidents. Whilst many global organisations are comfortable relying on existing internal resources, Australian organisations are more likely to outsource the investigation to specialists.

Whilst there are some organisations with a sufficient level of in-house expertise to manage all aspects of a fraud investigation, many do not, and in such cases external specialists are necessary. This is particularly the case in a business environment that is becoming ever more reliant on electronic communications and financial transactions. The ability to obtain electronic evidence and mine electronic data is a specialist task and a vital aspect to many investigations.

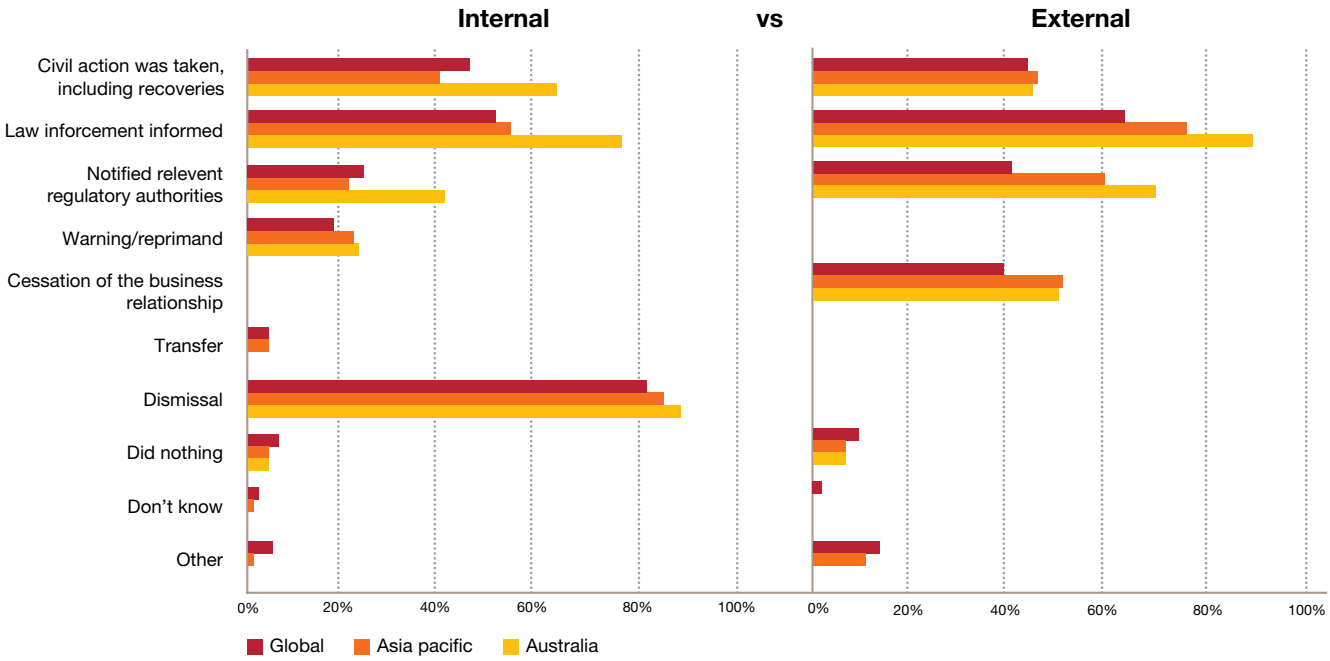
**When you identify an incident of potential fraud, which action(s) are you likely to take?**



# *Responding to fraud*

Our statistics show that Australia is leading its peers in terms of the seriousness with which it responds to detected cases of economic crime. Australian organisations are far more inclined to report the matter to law enforcement and take dismissal action against internal fraudsters.

**Fraudsters: Internal vs External**




This would also appear to be the case when it comes to regulatory reporting, with 67 per cent of Australian organisations notifying regulatory authorities about external fraud and 39 per cent for internal fraud. This compares to 39 per cent for external and 23 per cent for internal globally. Australian regulators are better informed than their global counterparts when it comes to reports of economic crime. This aspect is important when considering the impact of economic crime on regulation.

# *Procurement fraud in the mining industry*

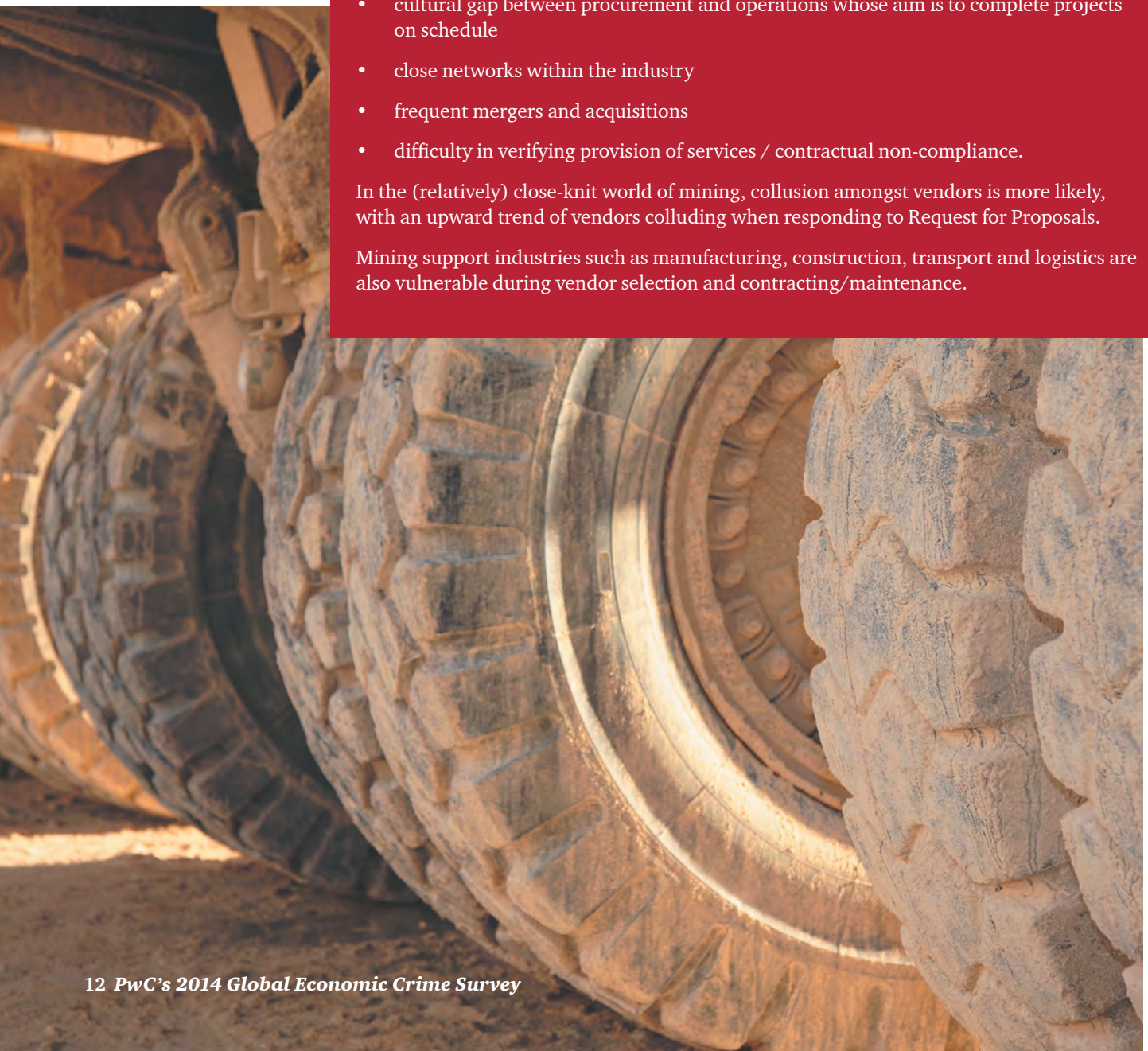
With the recent slowdown of the mining boom and a reduction in mining investment and funding, increased scrutiny over contracting has begun to reveal significant levels of procurement fraud. The key processes of concern are during vendor selection and contract monitoring. The large size of mining contracts (some worth billions) gives fraudsters the incentive, and opportunity, to perpetrate fraud as there is a greater chance it will go undetected given sizes and materiality of contracts.

Traditionally, it has been challenging to implement effective controls and prove contractual non-compliance over mining contracts due to a number of factors including:

- labour intensive operations
- geographical remoteness of operations
- lack of regulation
- cultural gap between procurement and operations whose aim is to complete projects on schedule
- close networks within the industry
- frequent mergers and acquisitions
- difficulty in verifying provision of services / contractual non-compliance.

In the (relatively) close-knit world of mining, collusion amongst vendors is more likely, with an upward trend of vendors colluding when responding to Request for Proposals.

Mining support industries such as manufacturing, construction, transport and logistics are also vulnerable during vendor selection and contracting/maintenance.



# On the take... the rise of procurement fraud

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.

At its most basic, procurement fraud is economic crime which occurs during the procurement life cycle. The offender may be an employee, owner, statutory board member, an official, a public figure or a vendor who was involved in the purchase or sale of services, goods or assets between organisations or individuals.

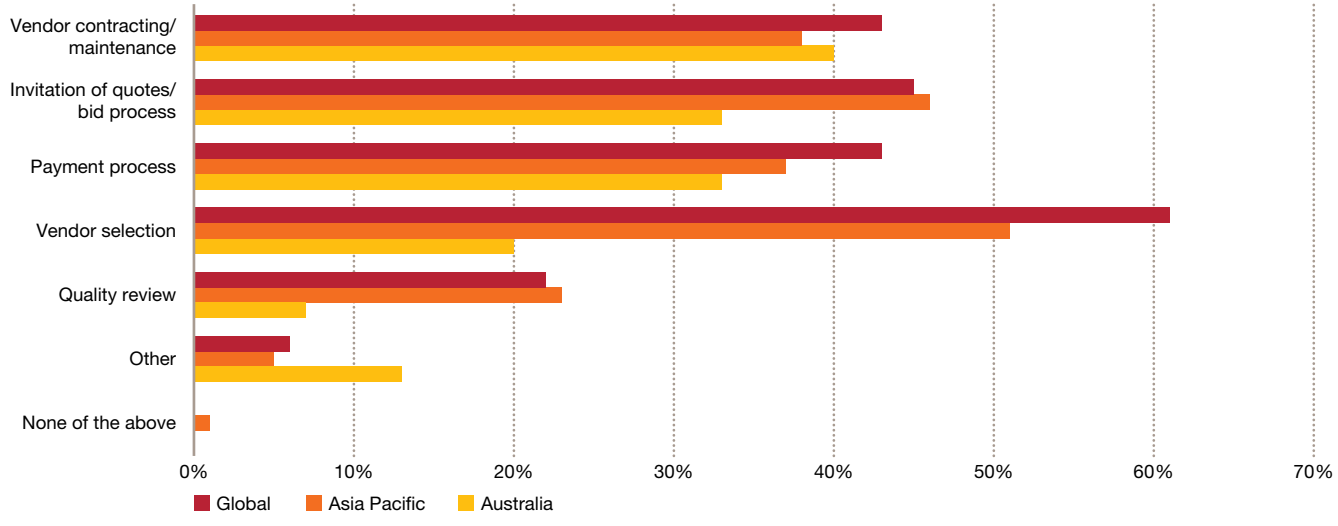
The procurement life cycle is a hotspot for fraudsters as it serves as one of the primary areas of expenditure for most organisations. The life cycle may be considered as follows:

**The procurement fraud lifecycle**


Procurement fraud is often complex to investigate because it can occur throughout the procurement lifecycle. The fraud may form part of the contract, the relationships with suppliers, be perpetrated by internal employees or a variety of other circumstances. Therefore procurement fraud can be difficult to identify, prove, quantify or prosecute. For Australian respondents, vendor contracting and maintenance was the primary place procurement fraud occurred. For our global counterparts it was during the invitation of quotes and bids process.

Increased awareness around procurement fraud in Australia has focussed around contracting in particular industries such as mining, energy and construction. Many organisations in these industries, after years of strong top line growth, are now more focussed on business costs and are scrutinising contractor relationships and payments. Procurement related frauds that have existed for many years are being discovered due to this closer scrutiny.

**Where did the procurement fraud primarily occur?**

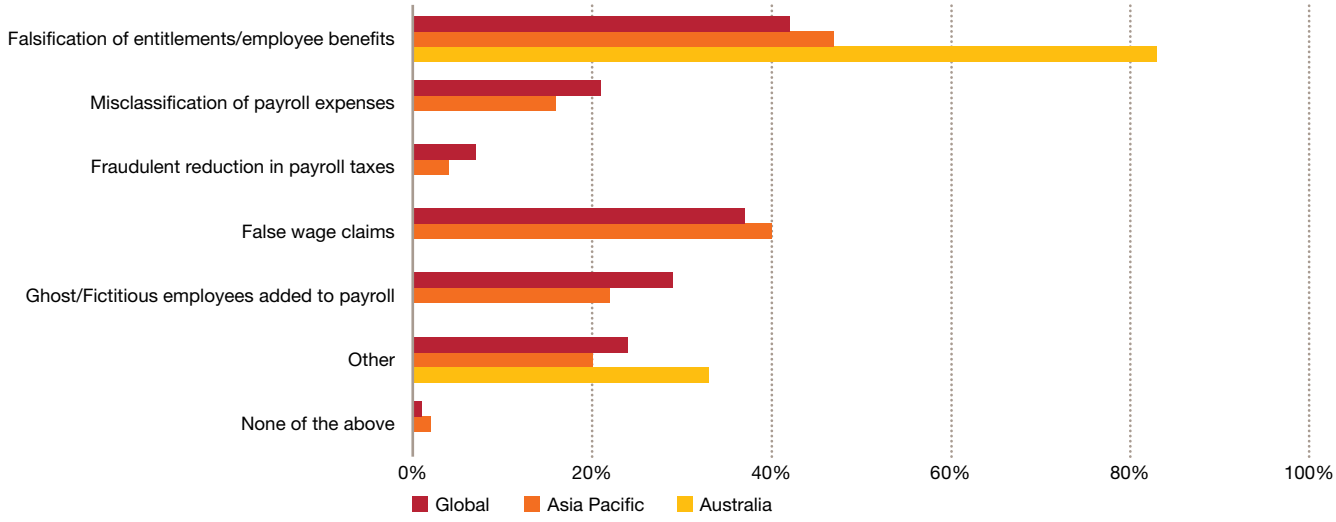


# Getting personal with human resources fraud

*According to the survey, human resources fraud represents 13 per cent of the fraud experienced by Australian respondents in the last 24 months. There does appear to be a rising global trend of human resources fraud with the global survey reporting 15 per cent of organisations surveyed experienced human resources fraud.*

As the name suggests, human resource fraud is concentrated within the employee benefits function and includes scenarios such as payroll fraud, ghost employees, pay-to-work and recruitment such as hiring friends and/or relatives, hiring unqualified individuals and falsification of documents. In Australia the number one type of human resources fraud experienced is the falsification of entitlements or employee benefits.

**Human resources fraud**




One of the many roles of a human resources department is to provide a safe working environment for an organisation's employees. The department often holds the primary responsibility for policy setting, including code of conduct and employee disciplinary policies. The behaviour of the human resources department, similar to the tone set by senior management, influences the cultural environment. Poor behaviour or the perception of lack of oversight by human resources can be taken as encouragement or approval for others within the organisation to display the same behaviour.

Due to this, human resources fraud may be an underlying indication of problems with organisational culture. Behavioural concerns, such as bullying and harassment may not themselves be an indicator of fraud. However, as part of our work with clients we have identified there is often a correlation between behavioural concerns and financial crime. A systemic culture which does not discourage this behaviour and a human resource department which is not seen to effectively handle these issues may hide an underlying tolerance or lack of management of fraud red flags.

# Think global, act global; dealing with corruption, bribery and money laundering

When asked which of the following three risks are perceived to be the highest risk for an organisation in doing business globally, Australian organisations ranked:

- corruption and bribery
- money laundering
- competition law / anti-trust law.

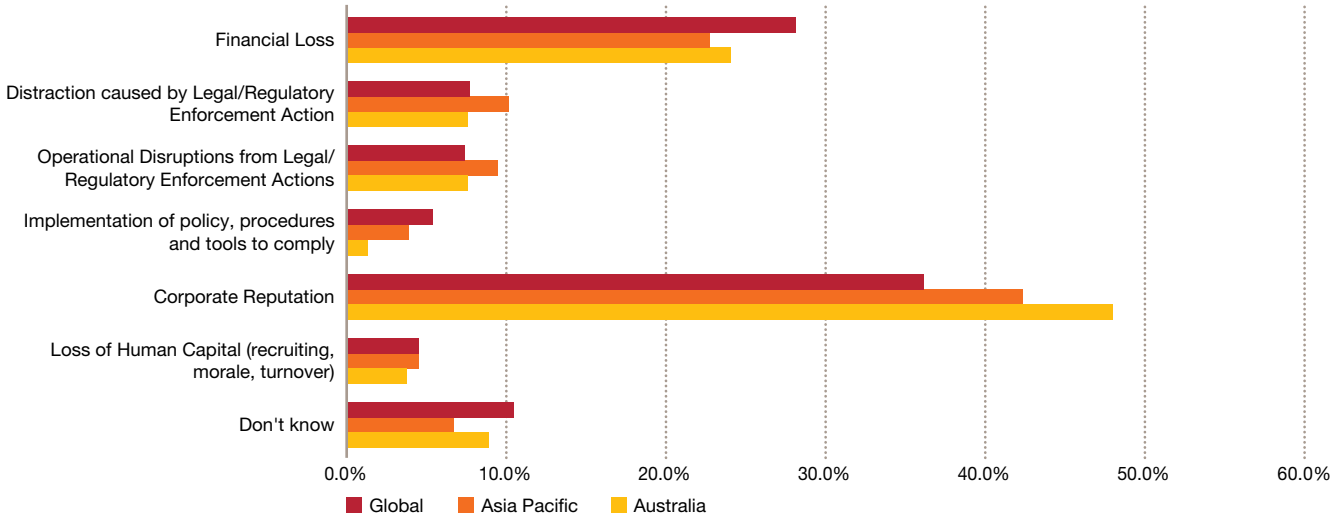
Many Australian organisations are looking for growth outside our borders and in a range of diverse economies, industries and cultures. Most are aware that the risks of doing business globally are different to those in Australia. The global focus on offshore bribery and money laundering, for example, is arguably more intensive than in Australia.

These global risks can have a major impact on an organisation's reputation, a fact not lost on Australian organisations based on the survey results. Most now appreciate that their activities offshore can have major reputational repercussions in all the markets in which they operate.

## *Offshore bribery, now knocking on your front door*

Business leaders now consider bribery and corruption to be a C-suite issue, as each act or instance can taint not only the individuals involved but an entire organisation, sometimes long into the future. Australian organisations consider the impact to corporate reputation as the most severe outcome if an act of bribery and corruption were exposed, higher than financial loss.

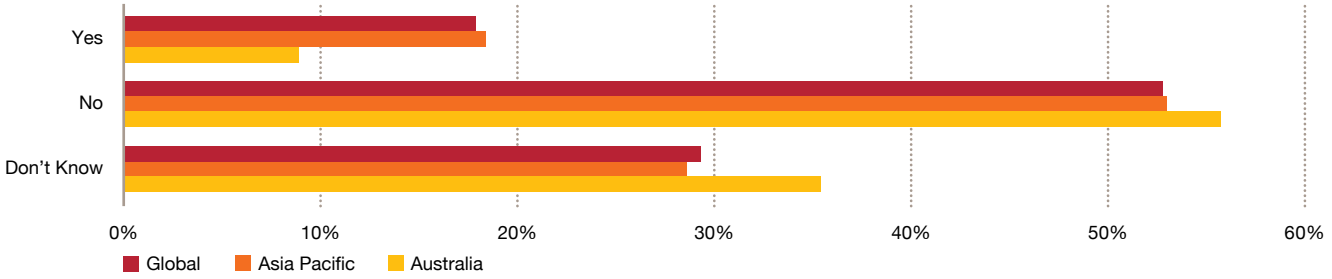
**With respect to corruption/bribery what do you perceive to be the most severe impact to your organisation?**



Almost a third of Australian organisations (32 per cent) currently have operations in markets with high levels of bribery and corruption and 29 per cent have pursued an opportunity in such markets.

In the past two years this has led to 6 per cent of organisations having lost over AUD 1 million dollars in relation to bribery and corruption.

**Has your organisation been asked to pay a bribe?**




Less than half altered their business plan and strategy in response to the potential corruption risk. Of the organisations that have altered their business plans and strategy in response to the potential risks when pursuing opportunities in high risk jurisdictions, the majority of them have done so by performing additional due diligence procedures.

Australian organisations are starting to recognise the need to take steps to reduce the risk of bribery and corruption.

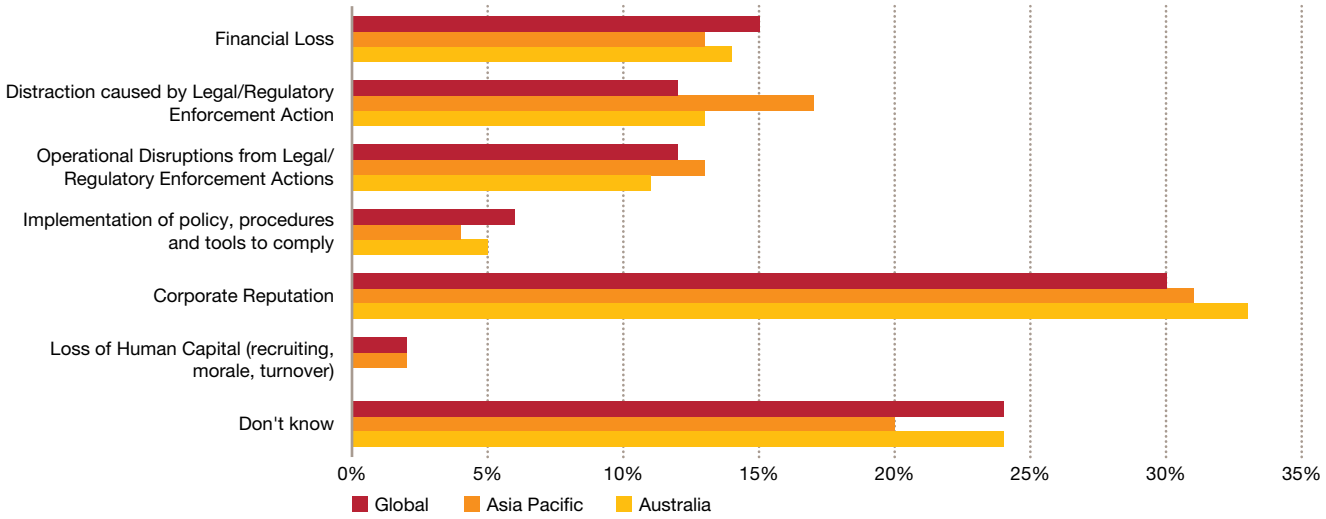
**Impacts of corruption from most to least severe with 1 being the highest risk**

# *Money laundering*

Money laundering or more specifically the risk of customers laundering money using your organisation is a major focus for global financial services organisations. Many global organisations have been levied with major fines for breaches of anti-money laundering legislation.

Australia has its own money laundering laws and its own regulator, AUSTRAC. AUSTRAC has indicated that its own enforcement activities will rise over the next few years and Australian financial services organisations that are subject to the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF) cannot afford to be complacent. Whilst there have not been major fines in Australia, the reputational impact of adverse enforcement actions or of a major laundering incident would be significant.

**With respect to money laundering what do you perceive to be the most severe impact to your organisation?**




Australian AML/CTF regulations require organisations to have a program to monitor for suspicious transactions and to identify customers - 'Know Your Customer' (KYC). Recent experience and global trends indicate it is the failure of KYC procedures that presents the most challenge to organisations and represents a major financial and reputational risk.

Outside financial services, although AML/CTF regulations may not apply, the due diligence principals underlying KYC remain an essential part of managing the risk of many different types of economic crime. For example, integrity checking around vendors, customers, agents and employees is a vital risk management technique, particularly for those operating offshore.

## *How does bribery and corruption manifest itself?*

Bribery and corruption is not only about the clichéd brown paper bag changing hands behind the site canteen. In our recent experience it can manifest in more subtle ways:

- breaches of procurement guidelines: direct appointment of subcontractors (plant, labour crane hire in particular), ambiguous contract arrangements, over ordering of stock for warehousing
- labour hire: inflated hourly rates, ghost contractors, under qualified resources, inflated manpower requirements, provision of unauthorised bonus payments
- plant hire: excessive plant on site, inflated maintenance agreements, ghost bookings, inflated plant performance, abuse of fuel privileges
- contract variances: significant instances/levels of 'day works' and other variances
- bullying and harassment: in order to facilitate above
- misguided loyalty: where labour and plant contractors show allegiance to transient management over the organisation themselves
- unjustified calls on bank guarantees and bonds: involving the compromise of a contract administrator.

### *Case Study*

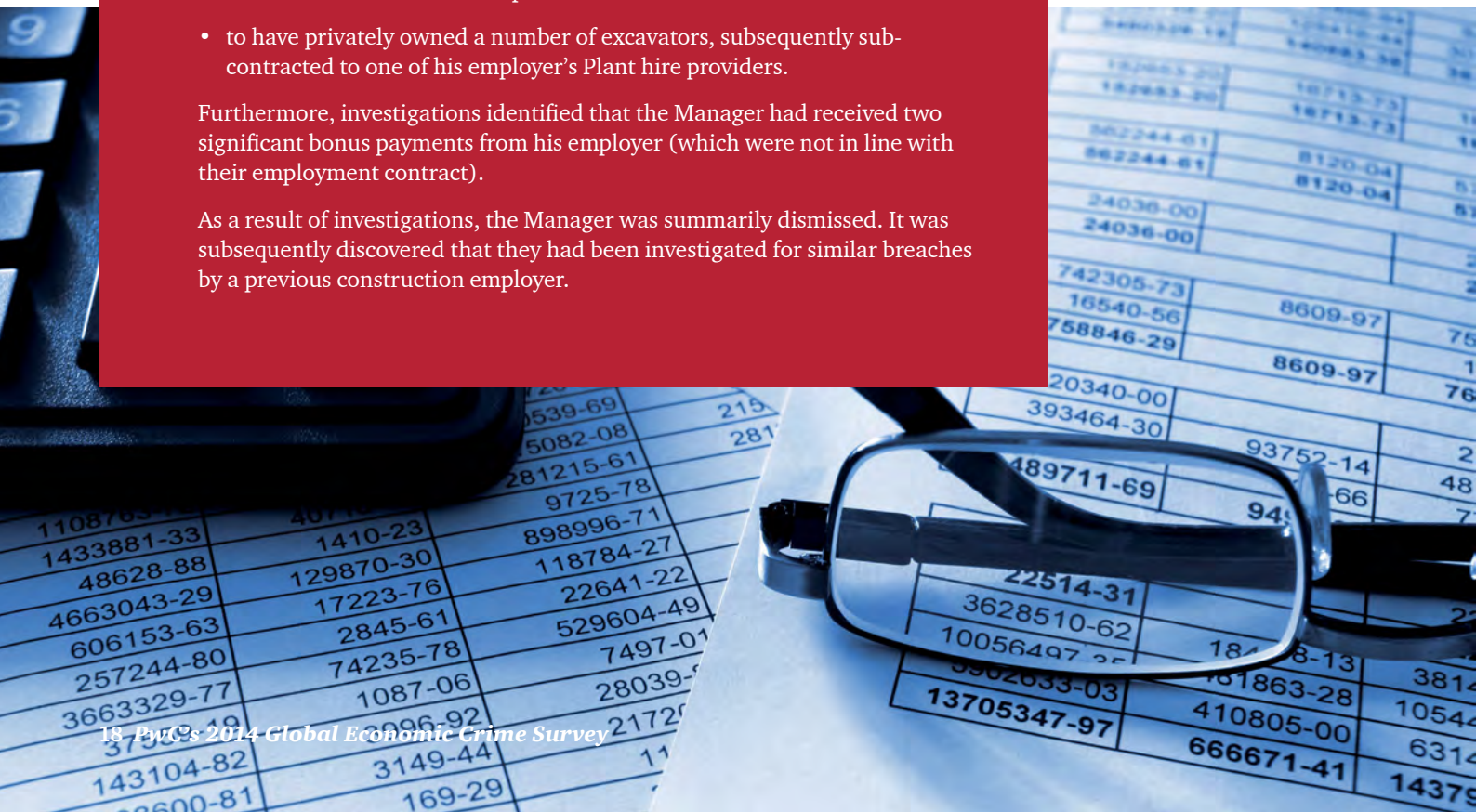
A senior Site Manager on a major construction project was found to have a non-arm's length relationship with a number of sub-contract plant hire companies.

They were found, through forensic accounting and electronic data analysis:

- to have accepted travel and entertainment (in breach of company policy) from a number of Plant hire providers
- to have privately owned a number of excavators, subsequently sub-contracted to one of his employer's Plant hire providers.

Furthermore, investigations identified that the Manager had received two significant bonus payments from his employer (which were not in line with their employment contract).

As a result of investigations, the Manager was summarily dismissed. It was subsequently discovered that they had been investigated for similar breaches by a previous construction employer.



## *Case Study*

An organisation, who was partner in a major mining project, received an anonymous allegation regarding the activities of a senior Engineering Manager. It was claimed that the Manager had set up their own labour hire company and was sub-contracting staff into the organisation at inflated rates.

Through forensic accounting, interviewing and data analytics, it was established that the initial contract (signed two years previous) allowed for two staff for a three month period. At the time of investigation, 20 contract staff had been assigned to the project, total invoicing was in excess of 30 times that originally approved. Supporting documentation was vague and incomplete.

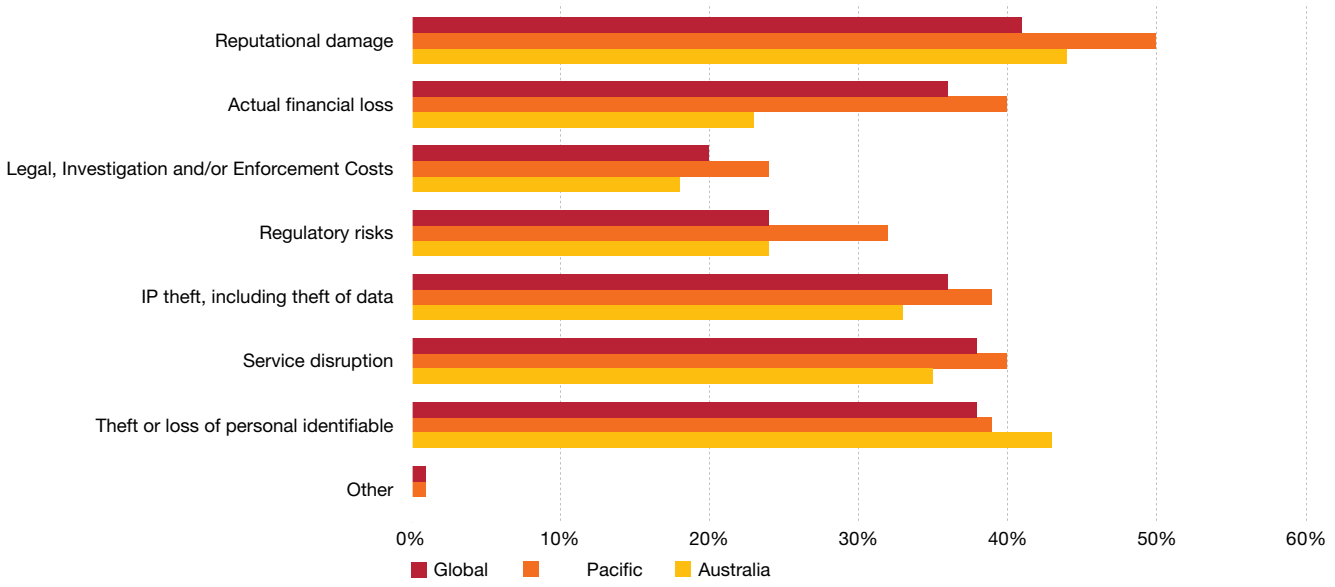
# Recap on Cybercrime

*This survey confirms the increasing impact of cybercrime on business, with 33 per cent of respondents reporting that they experienced cybercrime in the last 24 months, and one in ten organisations reporting financial losses of over AUD 1 million. However, the question of who is accountable for cyber across an organisation needs to be addressed. Recent cyber breaches have seen senior executives standing down as well as CIOs.*

There is increasing awareness of cyber risks among management and Boards. Almost three quarters (73 per cent) of Australian organisations identified that their perception of the risks of cybercrime to their business has increased over the last 24 months. Reinforcing this, 64 per cent of Australian CEOs in the 2014 PwC Australian CEO Survey said they were concerned about cyber-threats, including lack of data security. However businesses continue to treat cyber risks as an IT issue. Cybercrime is not just a technology issue, it is a whole of business issue.

Good security requires focussing on the most important data. Considering the huge amount of information that is now produced, safeguarding everything is not possible. The survey identifies that 43 per cent of respondents are concerned about the theft or loss of personal identifiable information and 33 per cent are concerned with Intellectual Property theft, including theft of data. 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.

**Recap on cybercrime**




Cybercriminals now understand the business environment, though many organisations do not fully understand the capabilities of cybercriminals and what they might target. The increasing use of technology in business processes has removed the traditional security perimeter as organisations adopt cloud, mobile and social technologies, and invest in third party business relationships. The digital ecosystem is complex and cybercriminals who come across an organisation with strong cyber defences will look to attack at the weakest link in the information supply chain, targeting third party suppliers and providers. Their risk is your risk.

# Where to from here

*It is positive that Australian organisations are well aware of economic crime risks and in many ways lead the world in terms of proactivity in fraud risk management. We believe this vigilance is key to preventing economic crime, or at least minimising its impact. It is likely that this attitude is reflected in the relatively high detection rate in the Australian survey results.*

Proactive organisations are those that look towards global trends, regulator activity, and technology to anticipate threats to their operations and mange that risk accordingly. Hopefully this report provides some insight into those trends and will allow Australian organisations to prosper in an increasingly risk aware business environment.

**Procurement fraud**

- Protect your business by implementing robust due diligence procedures when pursuing outside business opportunities and partnerships.
- When operating in high risk territories it's essential to have global compliance risk programs that are scalable.

**Human resources fraud**

- Australian organisations should not forget the human side of fraud and the impact organisation culture can have on the prevalence of fraud.
- The human resources department has an important role in leading from the front and to establish policies and procedures that effectively handle bad behaviour.
- Implementation of HR systems and processes that can detect and manage areas of concern such as employees falsifying entitlements / benefits.

**Bribery and corruption**

- Manage risk of doing business or expanding in to other countries through thorough due diligence and having flexible plans and strategy that can adapt to risk.
- The impact on corporate reputation as well as individual reputation means the Board and those employed by the organisation need to understand the potential risks and how to mitigate.
- Know your customer - integrity checking of vendors, customers, agents and employees to manage risk.

**Cybercrime**

- Cybercrime is a whole of business issue, not just technology but people and processes as well.
- Organisations can benefit from sharing their cyber-attack experiences with each so that the entire business community can learn and make Australia a difficult place for cybercriminals to operate in.
- Understand the types of cybercriminals and what information they might be trying to steal from your organisation so that you can effectively protect 'trophy data'.

## *About the survey*

The 2014 Global Economic Crime Survey was completed by 5,128 respondents (3,877 respondents in 2012) from 95 countries (78 countries in 2012). Of the total number of respondents, 50 per cent were senior executives of their respective organisations, 35 per cent represented listed companies and 54 per cent represented organisations with more than 1,000 employees.

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

# *www.pwc.com.au*

*For more information please contact:*


***Malcolm Shackell***
Partner. Sydney
+61 (2) 8266 2993
malcolm.shackell@au.pwc.com

***Jan Schreuder***
Partner, Sydney
+61 (2) 8266 1059
jan.schreuder@au.pwc.com

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

***Richard Bergman***
Partner, Sydney
+61 (2) 8266 0053
richard.bergman@au.pwc.com

***Duncan Taylor***
Director, Perth
+61 (8) 9238 3865
duncan.taylor@au.pwc.com

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

***Steve Ingram***
Partner, Melbourne
+61 (3) 8603 3676
steve.ingram@au.pwc.com

***Michael Cerny***
Partner, Melbourne
+61 (3) 8603 6866
michael.cerny@au.pwc.com

***David Harley***
Principal, Melbourne
+61 (3) 8603 0166
david.harley@au.pwc.com

***Gavin Moss***
Partner, Adelaide
+61 (8) 8218 7088
gavin.moss@au.pwc.com

***Stephen Hipkin***
Director, Brisbane
+61 (7) 3257 5154
stephen.hipkin@au.pwc.com





WL 127015285