Global Economic Crime Survey 2016 /
Australian Report

Embedding Resilience

Cyber threats, Anti-money laundering and Anti-bribery and corruption remains a persistent threat to Australian organisations

52%

of **Australian** respondents experienced economic crime, compared to the **2014** result of **57%**. The **global** rate is **36%** of organisations **(37% in 2014)**

30%

of **Australian** respondents experienced more than **100 incidents** of economic crime, compared to only **9%** of **global** respondents experiencing the same amount

30%

of surveyed **Australian** respondents suffered losses in excess of **USD 1 million** (approximately **AUD 1,399,468)**

pwc

www.pwc.com.au/gecs

Contents

2 *Introduction*

3 *Comparison Australia and Global*

5 *Cybercrime*

9 *Anti-Bribery and Corruption (AB&C), ethics and compliance*

10 *Anti-Money Laundering/ Counter-Terrorism Financing (AML/CTF)*

11 *Key findings*

13 *Prevention versus detection? Mastering the balance*

15 *Key contacts*

Introduction

I am pleased to present the Australian results of PwC's Global Economic Crime Survey 2016.

The Global Economic Crime Survey has been conducted every two years since 1999. It is one of the largest and most comprehensive surveys of its kind. It provides valuable insight and practical ideas on how organisations can continue their efforts to combat fraud and other economic crimes.

Economic crime remains a persistent threat to organisations in Australia, with an increasing focus on the digital and cyber landscapes. The digital environment has resulted in the evolution of economic crime, but the types of economic crime most commonly experienced by Australian organisations remains consistent with previous years: asset misappropriation, bribery and corruption, procurement fraud, cybercrime and accounting fraud. The landscape has changed but the threat remains. Organisations in Australia need to adjust by moving away from traditionally reactive detection methods to more sophisticated, proactive and embedded preventative and detective tools and techniques, such as we are seeing globally.

Resilience, while a fashionable buzzword, needs to become a part of the operational model for Australian organisations. Business leaders need to focus their efforts on combating Cyber threats, Anti-money laundering and Anti-bribery and corruption which remains a persistent threat to Australian organisations. Our consistently higher than the global average rate of incidence and cost of losses from economic crime reflects our reliance on doing what we have always done and a lack of increased investment in people, systems and tools.

We would like to thank all the Australian participants in the 2016 survey.

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

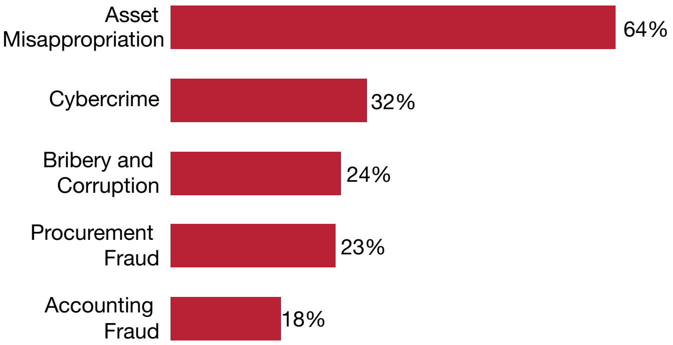
Comparison Australia and Global

A comparison of Australian organisations relative to global averages reveals some significant variations. While these in part reflect the maturity of the Australian market, they also show areas that should be of real concern to local organisations and provide an indication that many local organisations may not have adequately considered the cost and impact of economic crime and how they should deploy their resources.

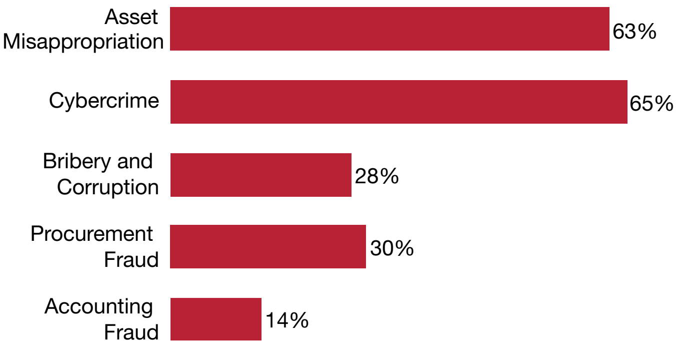
- **Exceeding the global average**: Although a slight reduction since the last survey (57%), more than half (52%) of Australian respondents have experienced economic crime in the last 24 months. This is significantly higher than the global rate (36%).
- **A heightened cyber threat**: Australian respondents have experienced cybercrime in the last 24 months at a much higher rate than the rest of the globe, overtaking asset misappropriation as the top economic crime experienced by organisations for the first time.

Q11 What types of economic crime has your organisation experienced within the last 24 months?

Global



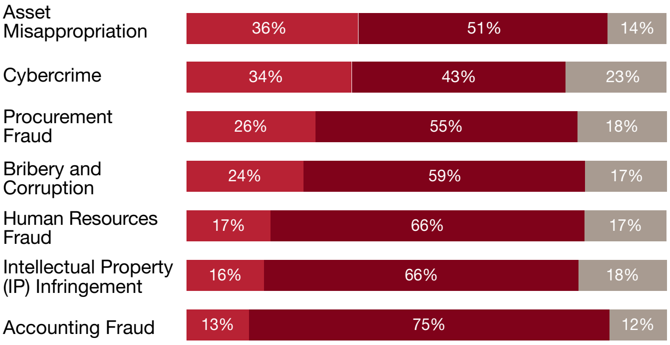
Australia



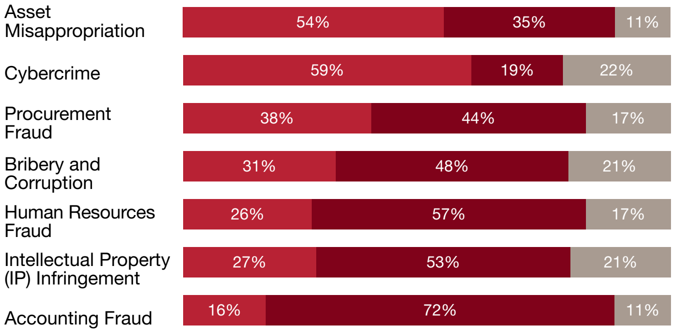
- **Volumes**: On average, Australian respondents reported experiencing more individual instances of economic crime in the last 24 months, with 30% experiencing 100 or more individual instances of economic crime.
- **The local perspective on the future**: Australian respondents believe they will continue to be impacted by the top five economic crimes at a higher rate than the rest of the globe.

Q14 How likely or unlikely is it that your organisation will experience the following economic crimes in the next 24 months?

Global



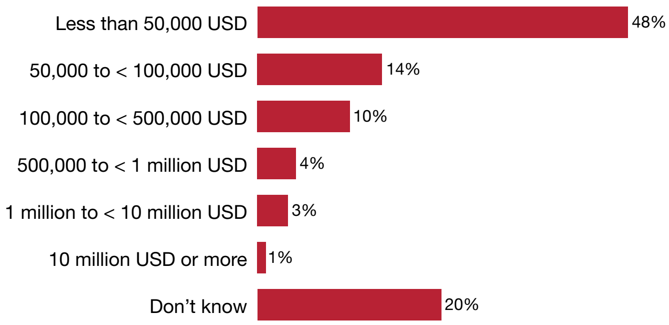
Australia



- **Higher spend on investigations**: Australian organisations are also spending more than the global average on investigations and other interventions. This likely reflects a combination of internal and external costs including reactive technology and data/evidence gathering.

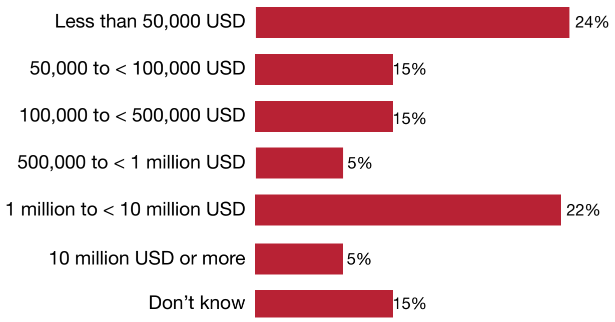
Q33 In financial terms, approximately, how much did your organization spend on investigations and/or other interventions as a result of economic crime (including AML & CFT if applicable) suffered in the last 24 months?

Global



Base global: 2,135
*Asked to respondents that have experienced economic crime at Q9

Australia



Base filtered: 41
*Asked to respondents that have experienced economic crime at Q9

> *"The Australian perception that their organisation will suffer from the impact of economic crime over the next two years is validated by the consistently higher rates, volumes and costs of economic crime experienced by Australian respondents."*

Cybercrime

"It's a digital business with digital criminals."

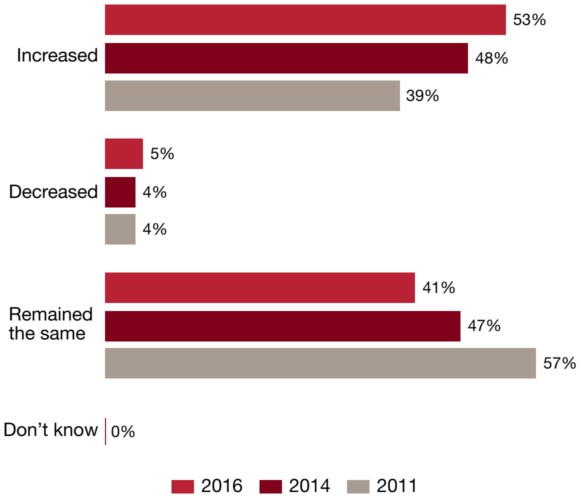
The increased use of new digital tools and platforms which enable organisations to connect with customers, suppliers and partners in real-time, is providing cybercriminals with new opportunities to target businesses. As a result, the last six years has seen the percentage of respondents who experienced cybercrime in their organisation move from being statistically insignificant in this survey to being the number one economic crime in Australia.

"The CEO gets it, but I am not sure the Board does."

Senior management realise cyber security is a serious risk with PwC's 19th Annual Global CEO Survey identifying cyber threats and the speed of technological change as top threats to growth. CEOs in Australia have major concerns, ranking these as the top two threats at 82% and 73% respectively, compared to 61% global. This is not surprising considering the reputational, operational and financial damages, with more than one in ten organisations in Australia reporting financial losses of over AU$1 million.

However, only half of respondents identified the Board as being proactive in requesting information regarding their organisation's state of readiness for cyber incidents. With almost six in ten Australian organisations expecting to experience cybercrime in the next 24 months, and 80% identifying an increase in their perception of the risks of cybercrime (up from 63% in 2012), how prepared are organisations to face ever-evolving cyber threats?

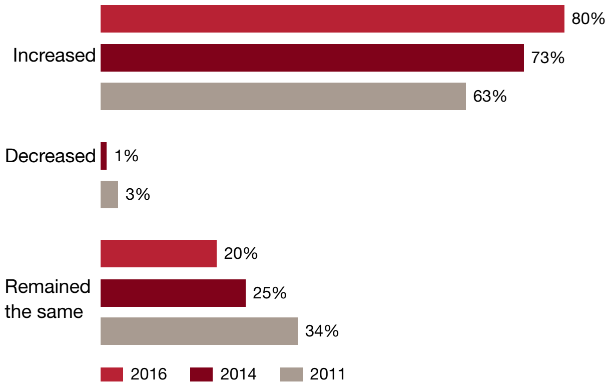
Q16 How has your perception of the risks of cybercrime to your organization changed over the last 24 months? – Historical view



Global Bases

Base 2016: 6,298 Base 2014: 5,128 Base 2011: 3,877

Note: 2011 question was asked regarding the last 12 months, in 2014 and 2016 it was asked regarding the last 24 months



Filtered Bases

Base 2016: 83 Base 2014: 79 Base 2011: 79

"We are getting better at responding, but there's a long way to go."

When a cyber incident occurs only 42% of respondents have a fully operational incident response plan and only 40% described their first responders as fully trained. An established, experienced and trained team of first responders drawn from the complete set of stakeholders (technical and non-technical) with the skills, knowledge and experience across an organisation are critical when responding to a cyber security breach. This team will need a specific set of skills:

- Business skills – making sure the right information is in place to make decisions and risks are pro-actively identified, assessed and managed
- Technology expertise – people who love technology and understand how it can be exploited for business use, but controlled to manage threats
- Forensic skills – taking a detailed approach to understanding why and collecting available evidence
- Malware analysis – understanding how malicious code is executed on a machine, where it came from, who it is targeted at and who is controlling it.

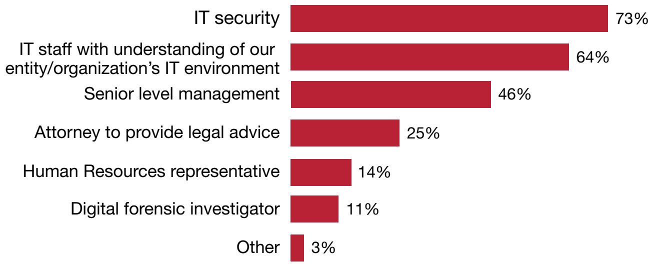
The increased level of awareness among management is opening up lines of communication between management and IT, and almost three quarters of organisations now include senior management in first responder teams. Other management areas are less represented, with only 36% including legal counsel and 20% including HR. Of more concern is only one fifth of these teams include digital forensic investigators, which may result in evidence being overlooked and limiting the ability to successfully prosecute.

Box for 'Plan & Prepare'

There is no off the shelf approach to incident response planning. Leading organisations have identified effective incident response begins with a robust planning process rather than a set of static plans and are integrating crisis management exercises into the incident response and cybersecurity strategy. This includes regular table top exercises examining different scenarios and assessing any gaps to improve the plans.

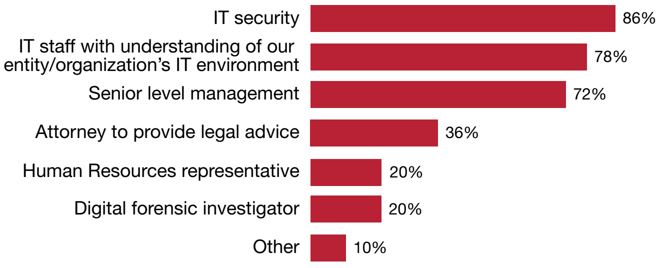
1. Understand the capabilities, motivations and objectives of threats.
2. Use intelligence to build realistic scenarios to test cyber defences.
3. Simulate cyberattacks against company networks.
4. Execute scenarios in order to cause realistic cyber pain on networks and document defence techniques and human reactions.
5. Understand and measure the team's responses, and refine the plan based on the results.

Q23 Which of the following types of specialists does yourfirst responder team include?



Base global: 3,829

*Those who selected "Yes..." at Q22



Base filtered: 50

*Those who selected "Yes..." at Q22

Game of Threats™ – A cyber threat simulation

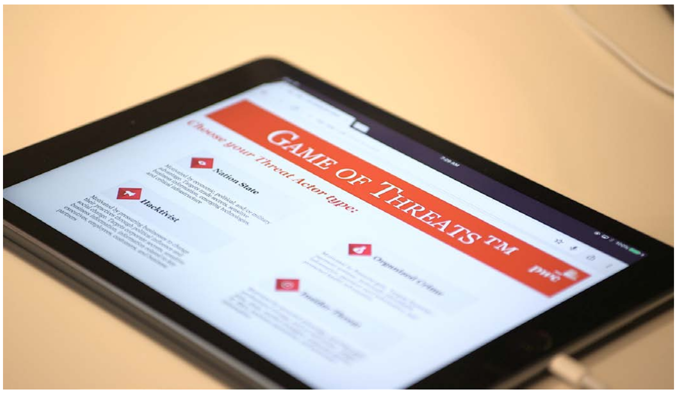
Game of Threats™ is a digital game that is designed to simulate the speed and complexity of an actual cyber breach. The solution integrates elements of gamification and game theory to provide an interactive client experience where a client team playing itself tries to defend itself from a of threat actors team (also played by company personnel). The game environment creates a realistic experience where both sides are required to make quick, high impact decisions with minimal information. At its core, Game of Threats™ is a critical decision making game that has been designed to reward good decisions by the players, and to penalize teams for making poor decisions. Players walk away with a better understanding of the steps they need to take to better secure their companies.

Fundamentally, Game of Threats™ was created to deliver a unique experience by allowing clients to feel pressure as they make fast paced decisions and to see potential consequences of their actions in real-time. Our game forces players to make choices about how to attack (if playing the threat actor) and defend (if playing the company) with limited information and to balance investment in capability and responding to the other teams' actions and plans.

PwC moderators facilitate a direct dialogue with clients about their choices during the game and provide on the spot feedback about strategy and decision-making. This approach elevates the impact of Client investments in cybersecurity awareness through real-time feedback on their selected actions, and a discussion about alternate responses and their potential outcomes.

Key takeaways from players:

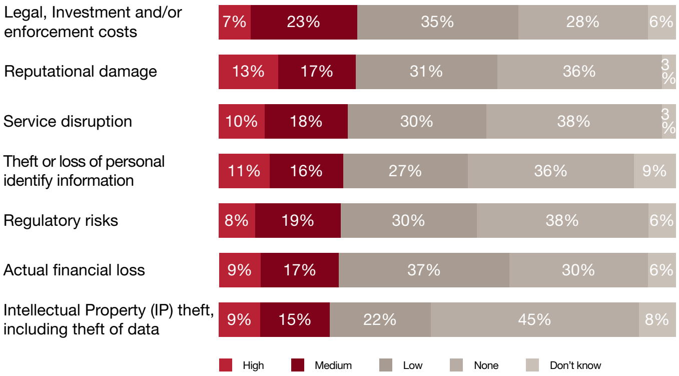
- Learn lessons about your company's ability to respond to a cyber attack
- Understand the potential ramifications and remediation options after an attack
- Understand what your company can do to prevent an attack
- Gain insight into the mindset of Threat Actors
- Learn key cyber security trends and terminology
- Spark a leadership discussion about your cybersecurity readiness



Other charts

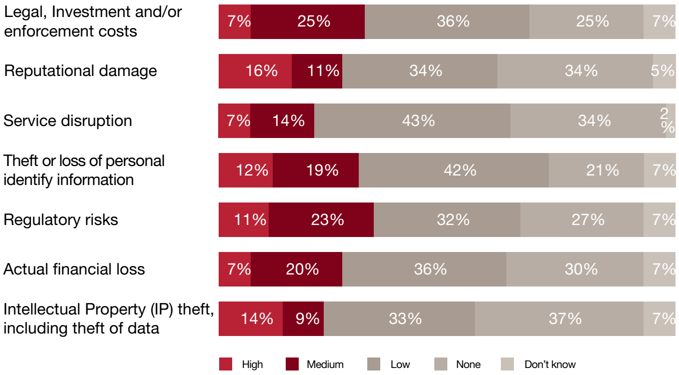
Q17b If cybercrime has affected your organization in the last 24 months, how would you rate the level of impact on the following aspects?

Global



Base global: 1,579 – 1,610
*Asked to respondents that have experienced cybercrime at Q17

Australia

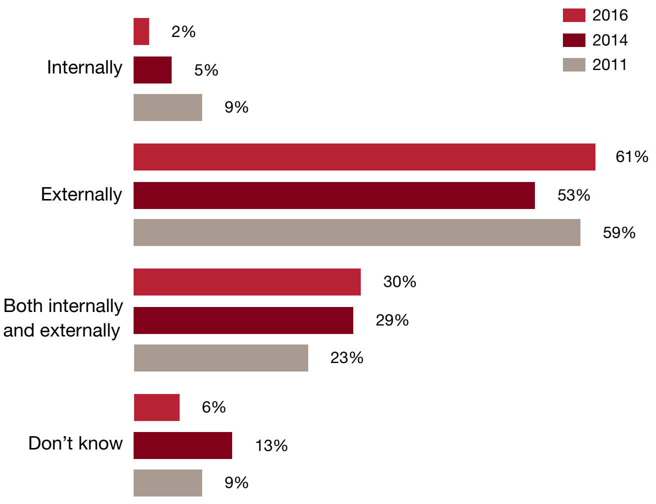


Base global: 43 – 44
*Asked to respondents that have experienced cybercrime at Q17

The Australian results

Q19 Where do you see the greatest cybercrime threat to your organization coming from in the next 24 months? – Historical view

Australian key findings

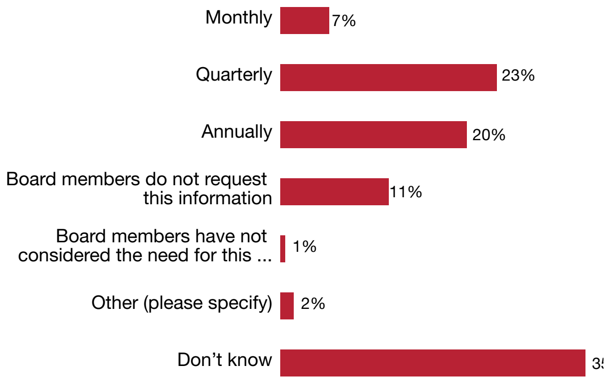


Filtered Bases

Base 2016: 83 Base 2014: 79 Base 2011: 79

Q20 How often do Board members request information regarding the organizations state of readiness to deal with cyber incidents?

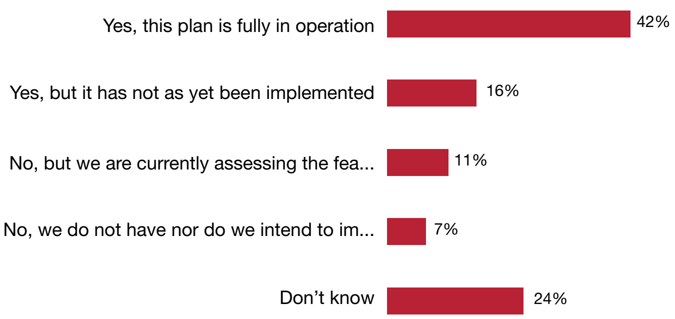
Australian key findings



Base filtered: 83

Q21 Does your organization have an incident response plan to deal with cyber attacks?

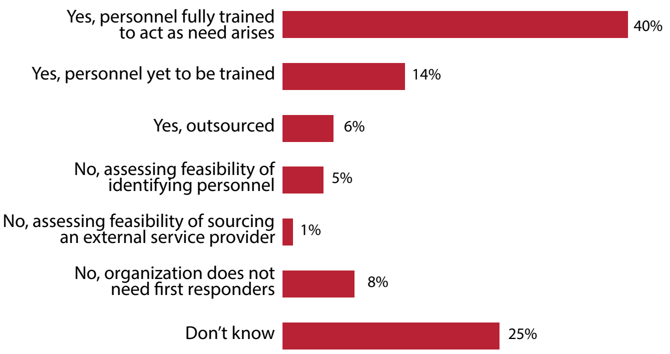
Australian key findings



Base filtered: 83

Q22 Has your organization identified first responders who can mobilise within a short space of time should a technology breakdown occur?

Australian key findings



Base filtered: 83

Anti-Bribery and Corruption (AB&C), ethics and compliance

Bribery and corruption continues to rate in the top four economic crimes experienced, and Australian organisations are predicting a higher likelihood of bribery and corruption in the next two years (31%) when compared with the global average (24%). From PwC's 19th Annual Global CEO Survey, the percentage of chief executives naming bribery and corruption as one of the top risks facing their organisation experienced – an increase, from 51% to 56%. These results come off the back of a number of highly publicised allegations and enforcement action reported in Australian media.

Australia continues to slide down Transparency International's Corruption Perception Index, now ranking outside the top ten (13th), and we have observed a growing disquiet concerning Australia's infrastructure for combatting bribery and corruption at a national level. State-based institutions continue to investigate allegations, but they are not designed to play a larger societal role around prevention. To combat an emerging lack of trust in business, Boards and company executives are increasingly looking to their ethics and compliance programs to take greater responsibility for both preventing incidents of bribery and corruption and strengthening organisational resilience.

The ability to identify and mitigate risks needs to evolve at a rapid pace. A risk-based approach to ethics and compliance – one that begins with a holistic understanding of your economic crime risk, and an understanding of where your compliance weaknesses are – is a must-have. From that position of clarity, you can create an effective program that mitigates those risks, and positions you for reaching your business goals. Better prepared organisation are looking to real time analytics solutions to assist with this.

Only 1 in 10 **Australian respondents** have not carried out a fraud and corruption risk assessment in the past 24 months and 37% of respondents have said they are conducting such a risk assessment annually.

Is your organisation doing enough to protect it from this continuing threat? Find out by answering five questions to see if your organisation meets the "gold standard" for managing bribery and corruption risk here:

Start the assessment online

Anti-bribery and corruption
Are you doing enough to protect your organisation?
Silver standard
Gold standard
Bronze standard

Anti-Money Laundering/ Counter-Terrorism Financing (AML/CTF)

Money laundering was experienced by **Australian respondents** at a significantly higher rate than the global average over the last 24 months (26% and 11% respectively) and continues to increase compared to the previous two surveys (approximately **16% in 2012 and 18% in 2014**).

"We've got more people, but it still isn't enough."

Globally, organisations are struggling to keep up with the pace of regulatory change and hire experienced AML/ CTF staff.

In Australia, we have seen an increase in investment and resources towards AML/CTF compliance; though there is a continuing challenge in funding and recruiting specialised financial crime expertise for the whole of the business, particularly in financial services. In the local market, there remains two key challenges a) securing funding for headcount from a reluctant organisation; and b) finding the right staff. While there have been very large punitive actions taken globally (often resulting in significant fines and remediation costs), Australian institutions have avoided the worst of these costs, producing a disincentive to invest in resources for many organisations.

"We need to invest in systems and tools."

A significant technology gap also remains. This is often as a result of legacy systems being maintained and re-purposed, data feeds being lost or misdirected as complexity grows, and a lack of sophistication in monitoring and detective activity. **Australian respondents** have underinvested in their AML/ CTF technology relative to their global peers.

Of note, over a third of Australian respondents reported that they had not taken any specific measures to limit their exposure to trade based money laundering activity as they believe that their business is not at risk. Trade based money laundering is a complex system of false documentation that enables criminals to earn and move value around the world under the guise of legitimate trade and is becoming harder to detect through traditional transaction monitoring systems.

Governments have imposed fines – and in some cases, pursued criminal actions – against financial institutions that have not implemented sufficient controls to monitor their global transactions. Regulators have indicated that they will have an increased focus on personal liability rather than just corporate liability. In short, they are looking for personal responsibilities around these failings. The days of individuals being protected by corporate settlements will soon be gone. As the American regulators[1] have made clear, individuals now face potential jail time if they are found to be complicit in illicit business practices or even substantive compliance failures.

Some financial institutions have come into the crosshairs of regulators in one country for illicit business practices in another. Often there are conflicts as to which country institutions are permitted to transact in while sanctioned by other countries.

Global survey respondents said that hiring experienced staff is the most significant challenge they face in the AML arena, tied at 19% with concerns on the pace of regulatory change. Unfortunately, the supply of talent continues to fall behind demand. Based on our discussions with clients and wider industry, churn among AML and compliance staff is high, and competition for top-shelf people is significant for both financial services and non-financial services companies.

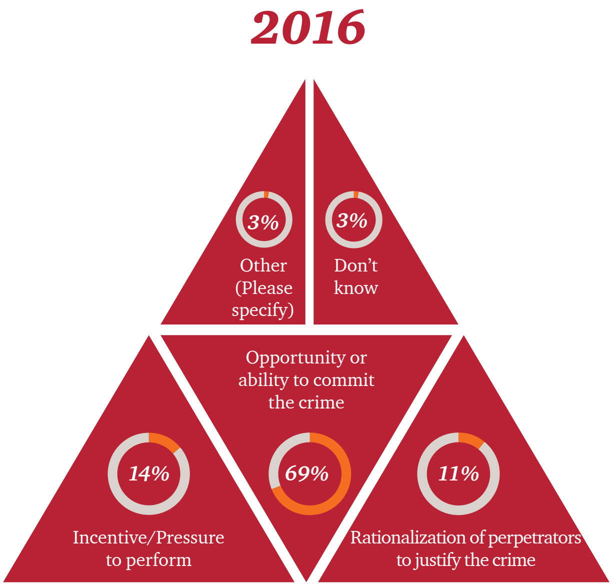
Risk assessments should be conducted on a periodic basis. They should be closely attuned to changed circumstances such as the operating environment, current global standards and practices and regulation in countries of operation. Assessments should also include the profiling of customers into different money laundering and terrorist financing risk categories.

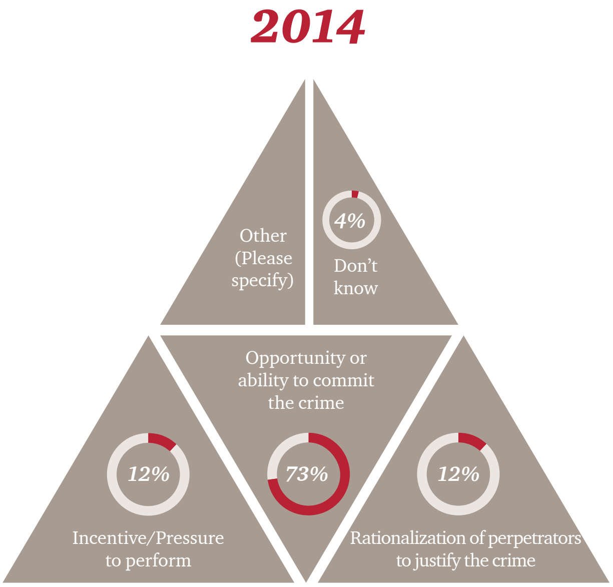
[1] New York Department of Financial Services, Office of the Comptroller of the Currency, Financial Crimes Enforcement Network (FinCEN) and the Office of Foreign Assets Control (OFAC)

Key findings

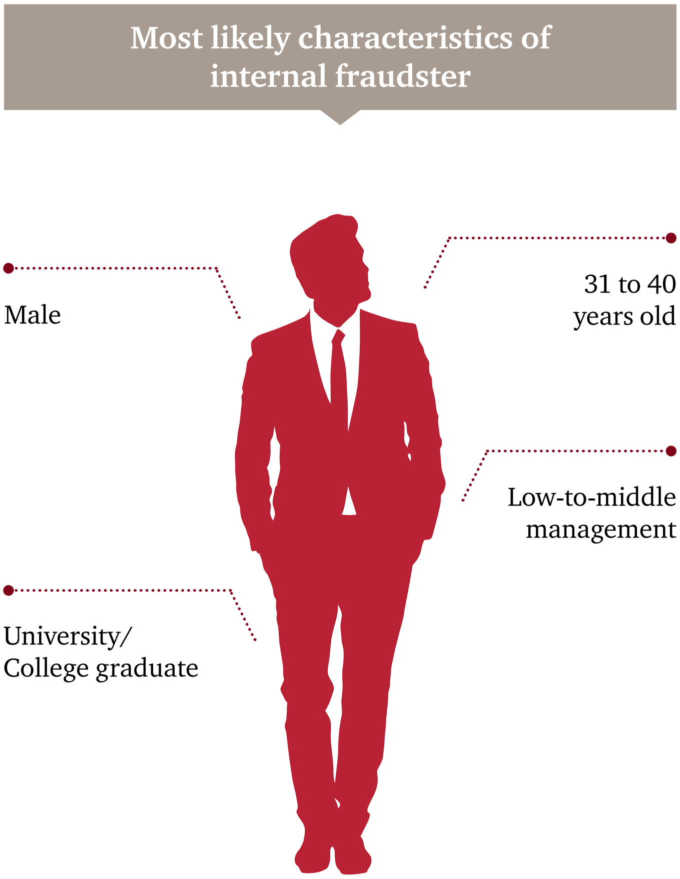
Profile of the fraudster

Seven in ten organisations believe that opportunity is the main driver of internal economic crime. This far outweighs the other two elements of the classic 'fraud triangle', which are incentive/pressure to perform and rationalisation of the crime.



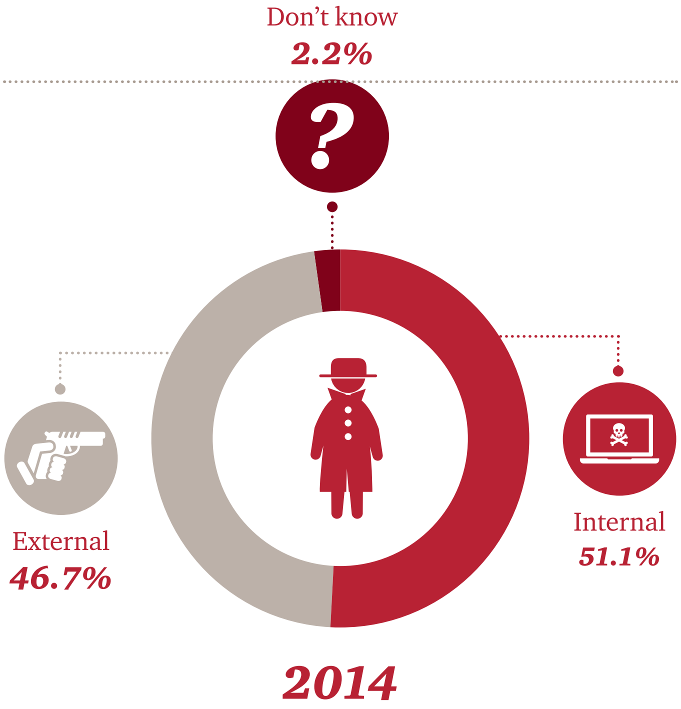


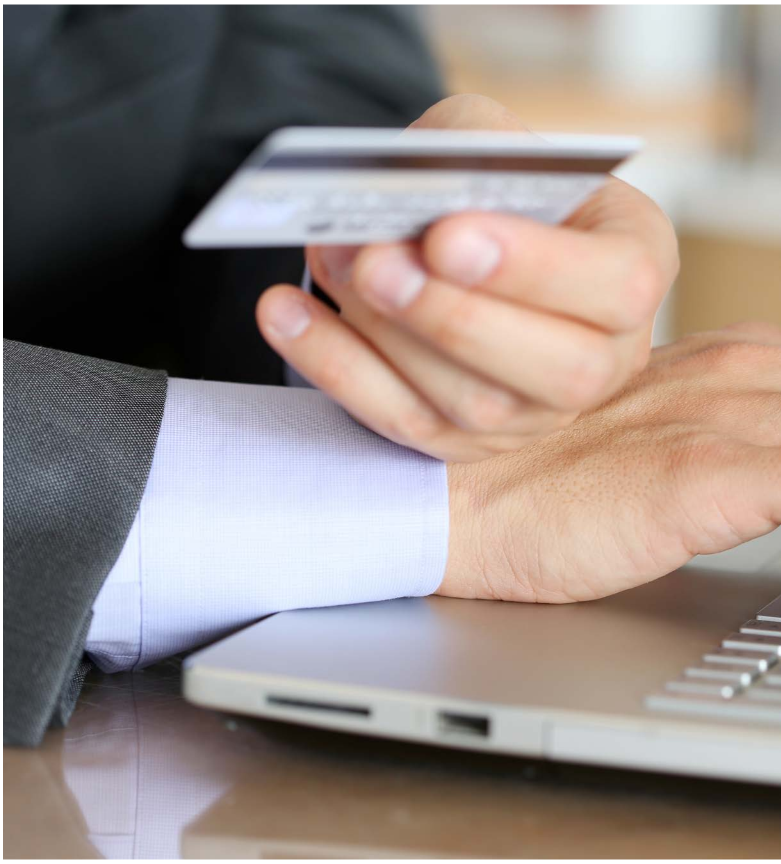
Q30 What was the profile of the perpetrator of internal fraud?

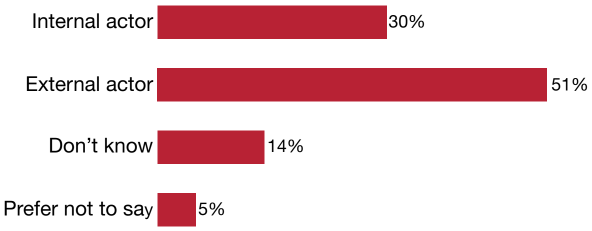

Most likely characteristics of internal fraudster
Male
31 to 40 years old
Low-to-middle management
University/ College graduate

While the profile of the internal fraudster has not changed significantly, the 2016 Survey results show a significant decrease in internal perpetrators to Australian respondents. It is likely that this reflects the increase in cybercrime instances since the last Survey which are often committed by persons external to an organisation. There is also a continuing upward trend in the likelihood that an internal fraudster is a university graduate (35% in 2014 to 47% in 2016), which likely reflects the increasing education profile of the workforce.

External versus internal fraudster







Base filtered: 43
*Asked to respondents that have experienced economic crime at Q9

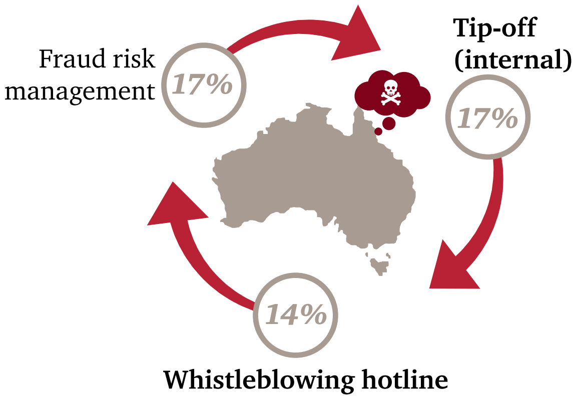
2016

> *“There is also a continuing upward trend in the likelihood that an internal fraudster is a university graduate (35% in 2014 to 47% in 2016), which likely reflects the increasing education profile of the workforce.”*

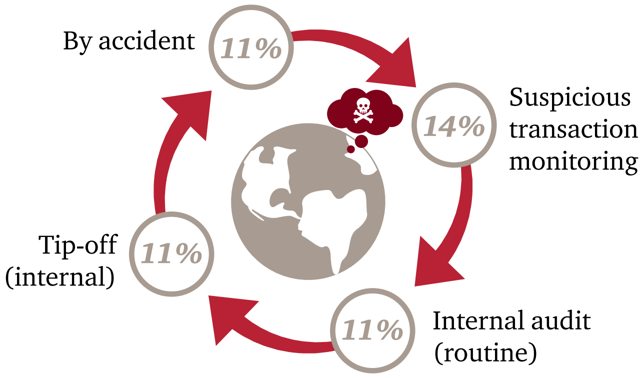
Prevention versus detection? Mastering the balance

Q31 Thinking about the most serious economic crime your organization experienced in the last 24 months, how was the crime initially detected?

Australia top three



Global top four



"We rely on our people telling us things."

When asked about the detection mechanism for the most serious economic crime events experienced by their organisation, Australian respondents said that they are more likely to rely on being told about a suspected crime than their global peers. There is a heavy reliance placed on internal tip-offs and whistleblower disclosures. This demonstrates the importance of establishing and maintaining avenues to report suspected economic crime by both internal and external parties, such as via whistleblower services. Australia needs to consider how we respond to (and protect) whistleblowers as we continue to rely on this detection mechanism. While the Australian Standards (AS8001 and AS8002) provide guidance on how organisations should effectively manage protected disclosures, the real world experience of whistleblowers does not always accord with the standards.

"IA takes care of the testing."

87% of Australian respondents reported they are relying on their internal audit (IA) function as part of their approach to assessing the effectiveness of their compliance programs. While internal audit is an important piece of the framework for assessing a compliance program's effectiveness, it may have an operational risk focus and not a specific fraud risk; it needs to be part of an on-going quality assurance (QA) function that is continually testing different elements of the fraud framework, preferably using real-time or near-time data feeds. In addition, the fraud risk profile has changed for many organisations, (for example, an increase in new frauds such as cybercrime) and it is imperative that the IA/QA framework is evolving to meet these challenges.

"I need to get proactive but it is hard to know where to start"

Ideally prevention should occur at the point of decision making. Fraud Risk Assessments should be integrated with management reporting and real-time monitoring in the business so that issues are detected and prevented in time.

Currently only 8% of respondents say they are using sophisticated internal monitoring approaches – such as data or predictive analytics – which are more difficult to circumvent. Today there are sophisticated and advanced tools – including big-data analytics capable of much more effective monitoring –that can help bring compliance closer to operations by handling a variety of structured and unstructured data.

In Australia, outside of transaction-monitoring systems (which are used primarily by financial sector clients), very few organisations are using these latest tools and technologies to help detect and prevent economic crime.

For many organisations, there is also more value in the 'small data' of risk assessments as well as the 'big data' space of transaction monitoring. These risk assessments should focus on organisational objectives and what data is available internally or externally that can validate how you are tracking to your objectives. To enable this, it is important to collect consistent and comparable data – which sounds simple, but often isn't. Understanding what data you have, how it flows and how it changes, can be a critical first step.

Currently only 8% of respondents say they are using sophisticated internal monitoring approaches – such as data or predictive analytics – which are more difficult to circumvent.

Key contacts

Malcolm Shackell

Partner, Forensic Services at PwC
+61 (2) 8266 2993

Cassandra Michie

Partner, PwC
+61 (2) 8266 2774

Jean Roux

Partner, PwC
+61 (3) 8603 0714

Richard Bergman

Partner, PwC
+61 (2) 8266 0053

Steve Ingram

Asia Pacific Cyber Lead at PwC
+61 (3) 8603 3676

Michael Cerny

Partner, Cyber at PwC Australia
+61 (3) 8603 6866

www.pwc.com.au