www.pwc.com.au

The new face of economic crime

‘Frenemies’, external threats and cyber now dominate economic crime in Australia

PwC’s 2018 Global Economic Crime & Fraud Survey: Australian Report

pwc

60%
of *economic crime* in *Australia* is committed by a *'frenemy'*

64%
vs
36%
external threats outweigh internal

29%
of organisations lost *$1 million* or more

The face of economic crime in Australia is changing – yet again.

More than half of all economic crime is now committed by people who do business with the organisation on a regular basis – employees, customers or suppliers. And for the first time since our Global Economic Crime Survey began in 1999, crime threats from outside the organisation now outweigh the risks from inside.

Despite commendable attempts to keep ahead of the evolving risk landscape, organisations are simply not winning. More than half were victims of economic crime over the last two years, and one in three lost more than $1 million. And with regulators ramping up enforcement and compliance activities, organisations face a 'perfect storm' of risk, costs and scrutiny from all sides. A new approach and a new mindset to dealing with economic crime are required.

This report outlines some of the key findings for Australian organisations from our 2018 global survey. We explore the changing nature of the threat environment and provide guidance on what organisations can do to respond.

About the survey

PwC's Global Economic Crime Survey is one of the largest and most comprehensive of it's kind. This year, we draw on data from more than 7,200 respondents across 123 different territories, including 158 respondents from Australia.

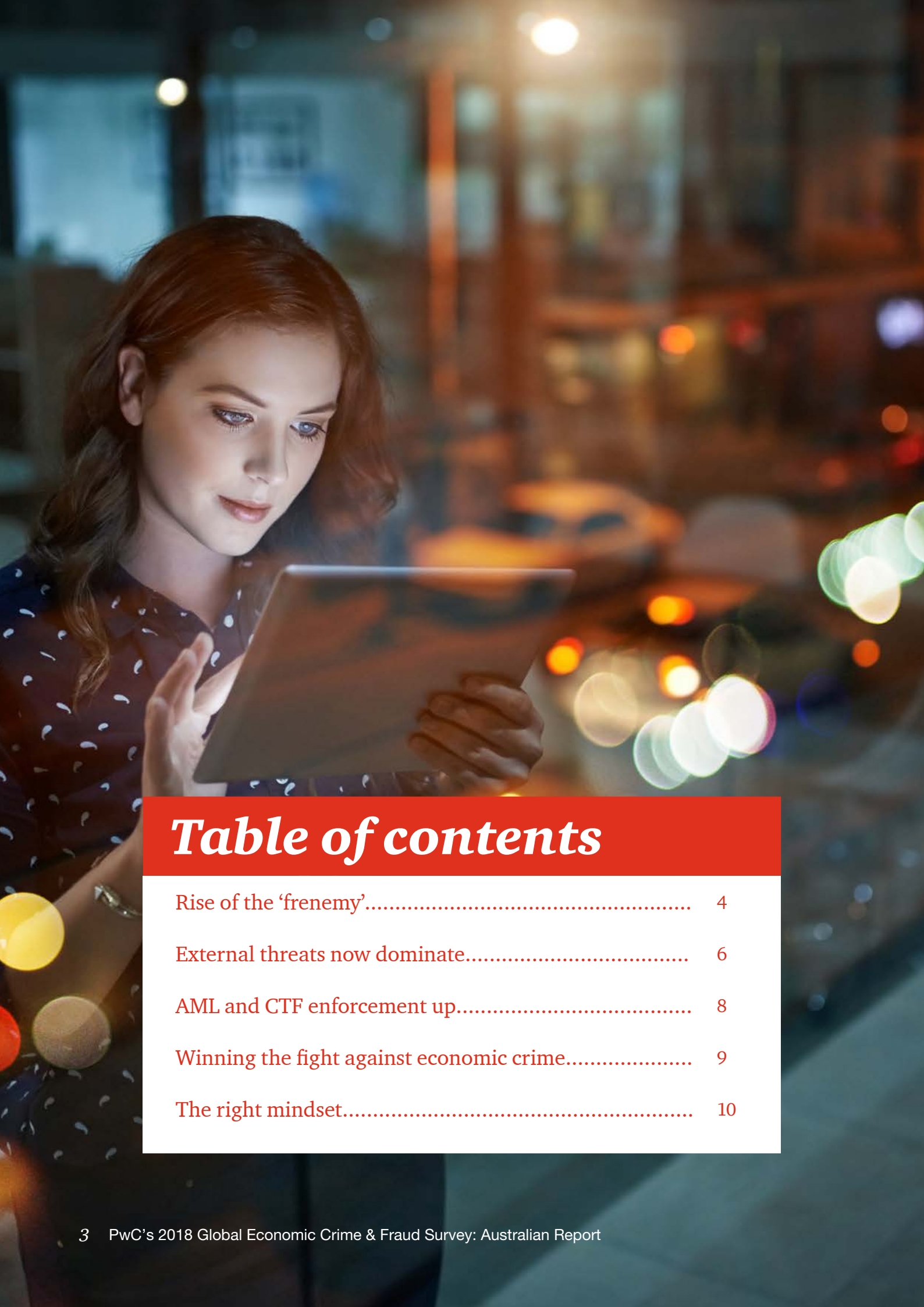
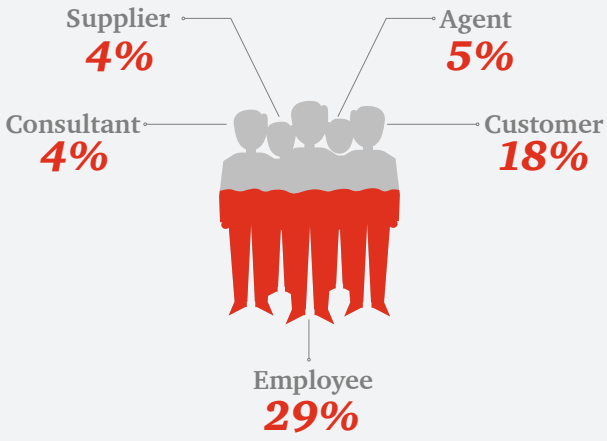


Table of contents

Rise of the ‘frenemy’

Most of us take it for granted that the people we do business with on a daily basis will do the right thing by us. But our most recent survey results point to a new and worrying trend that turns this assumption on its head.

The majority of fraud and economic crime in Australia – **60%** – was committed by someone close to the organisation, such as an **employee, customer, supplier, consultant** or **agent**; in other words, a ‘**friendly enemy**’. In fact, customer fraud is now the number one type of economic crime in Australia.



Organisations that have experienced customer fraud in the last 24 months:

So, what’s behind the rise in this type of economic crime? Why are employees, suppliers and customers biting the proverbial hand that feeds them?

One of the biggest drivers is the increasing availability of new technologies to facilitate fraud. For example, there is a rise in the use of ‘off the shelf’ editing apps to change documentation, make fraudulent IDs, credit card applications and insurance claims. People are also turning to the ‘dark web’ to source information about economic crimes and finding tools to help them. This easy access to technology is making the threat environment wider than ever.

Another driver is the increasing influence and sophistication of organised crime, who are continually finding ways to get closer to businesses. For example, do you really know the directors or key managers of your supplier companies? What about the past histories of business agents or consultants? Do you know if they have any links – however tangential – to crime syndicates?

Frenemy red flags – and what to do

It's natural to want to trust the people you work with closely. But as frenemies become more active in economic crime, you need to be aware of the risks and know how to manage them.

Here are some red flags that may signal your friend is in fact your enemy:

- If your employee or vendor is reluctant to complete the onboarding process and provide documentation in a timely, transparent and complete manner;
- If it's difficult to establish who is the ultimate beneficial owner of a third party you are working with;
- If corporate ownership structures are overly complex; and
- If verification relies on overseas translated documentation.

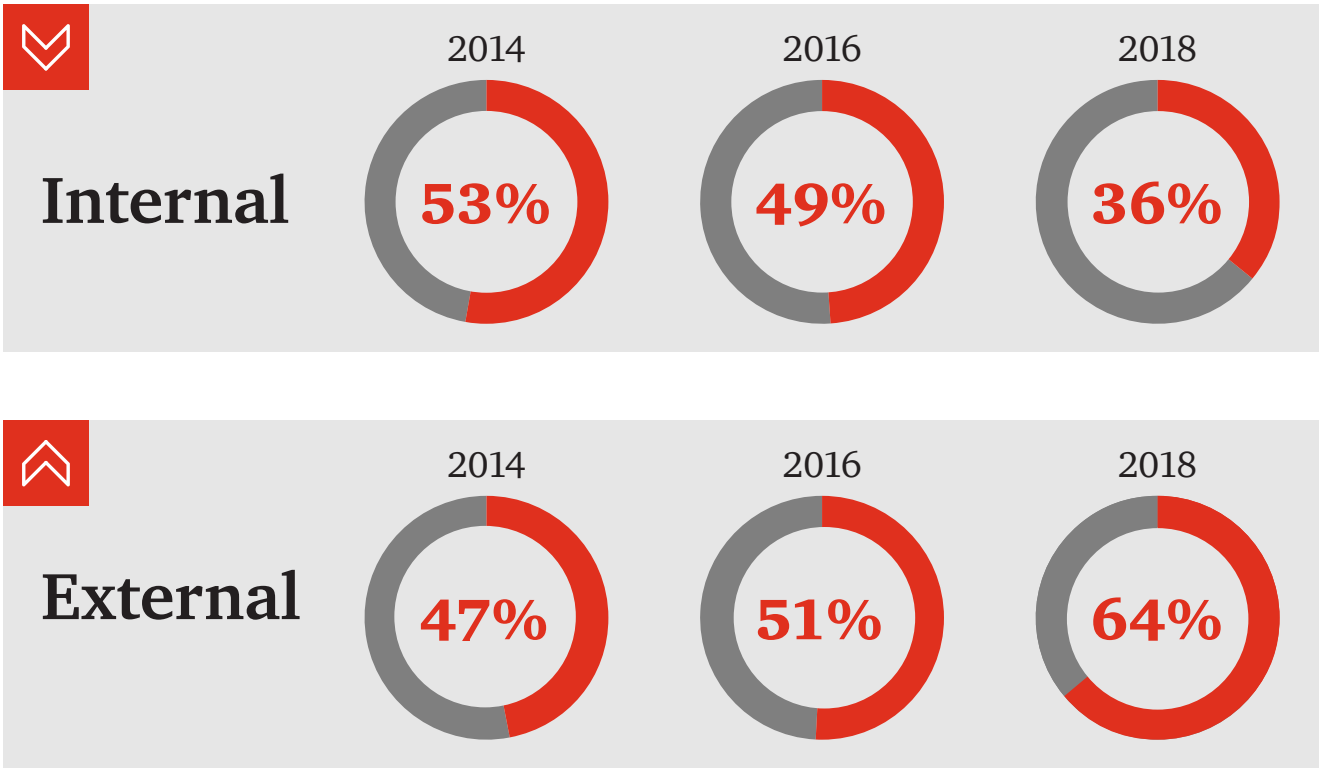
So what can you do to protect yourself from frenemies? The key is to be more active and alert at the beginning of the process – before you even become friends – rather than when something goes wrong. This means better background checks, better 'know your customer' (KYC) processes where required, and better due diligence before working with any new third party.

External threats now dominate

In addition to the rise of the frenemy, our survey highlighted another significant change in the economic crime landscape in Australia: the growing dominance of external threats. Four years ago, less than half of all economic crime came from outside the organisation, from places like hackers, organised crime or customers. Now, external sources account for closer to two-thirds of this activity.

Once again, technology is one of the key drivers behind this shift. Like their frenemy counterparts, external criminals are taking advantage of the dark web and readily available technologies to commit fraud and crime. And if these actors are part of an organised crime syndicate, they can also bring significant scale to their nefarious activities.

Sources of economic crime in Australia



Of course, the rise in external actors does not mean 'internal' risks have disappeared; they remain as real and as urgent as ever. But organisations need to be alert to the changing nature of the threat environment so they can adopt the necessary controls to manage the evolving risk accordingly. Unfortunately, many are lagging behind. More than 40% of companies we surveyed have not assessed the risk of fraud in the last two years, which leaves them increasingly vulnerable to new and emerging forms of economic crime.

Cybercrime: your biggest competitor?

Of all the external threats, cybercrime is firmly at the top of the list. In the last two years, almost half (43%) of Australian organisations we surveyed said they had suffered a cyber attack. However, the number is probably much higher; we see at least one new attack every fortnight. And it's likely only to get worse. Both in Australia and globally, firms expect cyber be the most disruptive economic crime over the next two years, and CEOs say it's the number one threat to their organisation's growth prospects.

Part of the reason cyber poses such a significant threat is because today's cybercriminals are as savvy, professional and organised as the businesses they attack. In fact, cybercrime can almost be considered an 'industry' in its own right, given the scale of its operation and the sophistication of its methods. Think of it as the biggest competitor you never knew you had.

In Australia, the five most common types of cyber attacks were:

Phishing
48%

Malware
39%

Network scanning
24%

Brute force attack
15%

Man in the middle
10%

On top of this, cyber thrives on the same kinds of technologies that organisations are using to drive growth. For example, while the adoption of cloud computing and the Internet of Things can lead to improved efficiencies and innovations, they also increase the number of 'attack surfaces' for cybercriminals to target. This does not mean that organisations should retreat from technology. Instead, they need to design, build, test and deploy with cyber in mind.

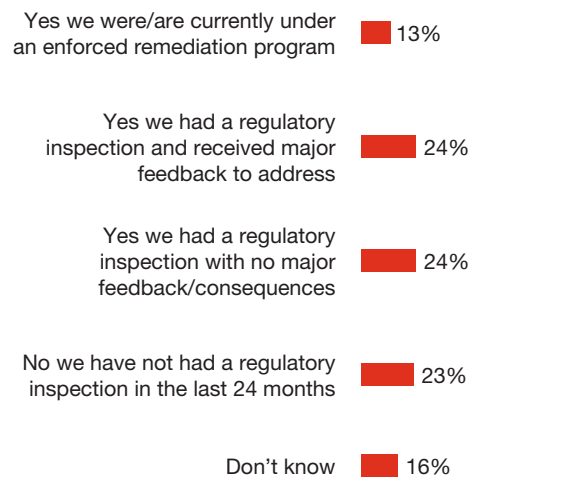
So what are organisations doing about cyber? Unfortunately, not enough to stay ahead of the threat. In Australia, almost half (48%) have not completed a cyber vulnerability assessment, while over one-third (36%) don't have a cybersecurity plan in operation. Without these 'basics' in place, organisations will find themselves not only highly vulnerable to a successful cyber attack, but poorly prepared to respond when the inevitable happens.

AML/CTF and anti-bribery enforcement up

In the last two years, regulators have significantly ramped up their enforcement of anti-money laundering (AML) and counter-terrorism funding (CTF) legislation in Australia. Of the fifty five organisations in our survey that are subject to the these rules, more than three-quarters (77%) had experienced regulatory enforcement or inspection. But worryingly, only 59% had completed a risk assessment around AML/CTF. Considering that fines far exceed the cost of compliance, this heightened risk of enforcement means affected companies need to make sure they are taking their responsibilities around this issue seriously.

On top of this, companies doing business overseas may also need to consider the impact of new anti-bribery and corruption legislation due in 2018. The draft laws are expected to introduce a range of new offences, including a new corporate offence of failing to prevent foreign bribery. This provision means that companies would be automatically liable for bribery by employees, contractors and agents (including those operating overseas), except where they can show they had a proper system of internal controls and compliance in place to prevent the bribery from occurring.

Has your organisation experienced any regulatory enforcement/ inspection about AML/CTF in the last 24 months?



Base: 62

Australia

Join PwC's Network of Cyber & Forensics Professionals

Building Transparent Businesses is a network of Cyber & Forensics professionals, a community of experts and organisations coming together to learn, share knowledge and help build trust and transparency within the business community.

The network will give you access to experts in the field, the latest PwC thought leadership, skill building and networking events. The program will focus on preventing, detecting and investigating the risks of fraud and financial crime in a unique, differentiated way to reduce their impact on your business and the business community.

Join the network today at https://www.pwc.com.au/btbnetwork

Winning the fight against economic crime

With economic criminals continually developing new ways to defraud and steal, organisations must be agile and adapt to stay ahead. Here are some questions to think about to help you address three of the biggest challenges.

Frenemies

1. Have you defined economic crime and communicated it across the business?
2. Do you really know who works for you? Have you completed background checks, spoken to previous employers, validated education, taken references?
3. Do you know who you are working with? Who are the owners, directors and key management? Do they have any criminal convictions, undischarged bankrupts, disqualifications as a director, adverse media, or legal proceedings?
4. Does your supplier have a third party risk management framework and due diligence program?

Cybersecurity

1. Have you completed a cybersecurity risk assessment?
2. Have you developed a cyber-incident response plan?
3. Are you prepared for the mandatory Data Breach Notification Scheme?

Financial crime regulation (including AML/CTF)

1. Do you have a register of commitments made to all regulators and are you tracking it?
2. Have you assessed regulatory gaps or non-compliance and do you have a process to identify and respond to changes in the financial crime regulatory landscape?
3. How comfortable do you feel that your financial crime policies and procedures are implemented in practice?

The right mindset

Traditional approaches to fighting economic crime are becoming less and less effective, and at some point in the future may cease to work at all. By adopting the right mindset, however, organisations can recover the upper hand:

1. Treat economic crime holistically – consider your entire threat environment including frenemies, internal and external threats in an integrated way
2. Focus on prevention – understand your vulnerabilities and how they are continually changing over time
3. Commit resources – only 25% of organisations surveyed had a dedicated team to address economic crime
4. Leverage advanced technologies – less than 15% of organisations surveyed were using machine learning, natural language processing, natural language generation, voice recognition, predictive analytics or artificial intelligence to prevent and detect fraud
5. Keep investing in people – machines can only do some much, you also need to address human behaviours that increase your organisation's vulnerability to crime.

Let's continue the conversation

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

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

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

Jean Roux
Partner
jean.a.roux@pwc.com
+61 (3) 8603 0714

Peter Forwood
Partner
peter.forwood@pwc.com
+61 (3) 8603 0664

Jason Knott
Partner
jason.knott@pwc.com
+61 (8) 9238 3418

Join PwC's Network of Cyber & Forensic Professionals

Building Transparent Businesses is a network of Cyber & Forensic professionals, a community of experts and organisations coming together to learn, share knowledge and help build trust and transparency within the business community.

Join the conversation around 'Building Transparent Businesses' at www.pwc.com.au/btobnetwork

© 2018 PricewaterhouseCoopers. All rights reserved.

PwC refers to the Australia member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

Liability limited by a scheme approved under Professional Standards Legislation.

At PwC Australia our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 236,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.au.

127061392