



2020

Fighting fraud: A familiar foe in unfamiliar times

PwC's Global Economic Crime and Fraud Survey: **Australian findings**

www.pwc.com.au/gecs2020



The ongoing battle against fraud and economic crime

For over 20 years, PwC's Global Economic Crime and Fraud Survey has tracked companies' experience of the full – and expanding – array of crimes that fall into this category. This year our global research covered more than 5,000 organisations across 99 countries. The top-line finding? Nearly half of the respondents told us they had experienced a fraud in the past 24 months – suffering aggregate losses totalling some AU\$60 billion (US\$42 billion) as a result.

The COVID-19 pandemic has given rise to many challenges for organisations trying to manage disruption and uncertainty. Both internal and external fraud are particularly prevalent during downturns. Disturbances in business processes, controls and working conditions give malicious actors opportunities to commit fraud, while pressure on businesses and individuals alike can motivate fraudsters to act. As economies continue to contract, it has never been more important for organisations to understand the key fraud risks that are threatening their organisations and put in place measures to minimise those risks. The survey findings provide valuable insights for Australian organisations trying to emerge stronger from the current crisis.

Global highlights



Fraud

For over 20 years PwC's Global Economic Crime and Fraud Survey looked at a number of crimes, including:

- Accounting/Financial Statement Fraud
- Anti-Competition/Antitrust Law Infringement
- Asset Misappropriation
- Bribery and Corruption
- Customer Fraud
- Cybercrime
- Deceptive Business Practices
- Human Resources Fraud
- Insider/Unauthorised Trading
- Intellectual Property (IP) Theft
- Money Laundering and Sanctions
- Procurement Fraud
- Tax Fraud



Fraud is a challenge that's both constant and continuing to evolve – but which is showing no sign of reducing any time soon. Our 2020 study confirms that companies in Australia must remain as vigilant as ever.

Companies in Australia appear to have suffered less fraud than their counterparts elsewhere in the world in the past two years: just 35% of Australian respondents said they had experienced fraud, well below the global figure of 47%.

At first sight this result looks like good news. But is it that Australian companies are suffering fewer frauds, or just not detecting them as quickly or rigorously?



Almost
one fifth
of Australian respondents
were asked to **pay a bribe**
in the past 24 months

Source: PwC Global Economic Crime and Fraud Survey 2020

There's no room for complacency

Other findings suggest this gap in reported fraud may not simply indicate a lower level of fraud in Australia. Instead, it may partly reflect a lower overall level of maturity and investment in the fraud programs run by Australian companies. As we will highlight later, this includes a lower focus than elsewhere in the world on fraud detection and training, and on implementing formal procedures in areas like third-party due diligence.

A comparison with the global figures reveals three major opportunities for Australian companies to improve their fraud programs:

1. **Governance and resources:** Just 8% of our respondents in Australia – compared to 14% globally – have dedicated anti-fraud resources who are compliance experts and whose budget needs are prioritised. Only 15% of respondents globally indicated that they had no governance, resources or budget for addressing fraud, this figure leapt to 32% among Australian organisations.
2. **Risk assessment:** Some 63% of Australian respondents do not have a formal risk assessment for fraud in place, compared to 47% of global respondents.
3. **Investigations, disciplinary measures and incentives:** Over one in four (26%) respondents in Australia do not have investigations, disciplinary measures or incentives processes in their overall fraud programs, compared to less than one in seven (14%) globally.

At the same time, further findings underline that Australian companies cannot afford to be complacent about fraud. For example, bribery and corruption remains a significant problem, with almost one Australian respondent in five – some 19% – reporting that they've been asked to pay a bribe in the last 24 months.



The perpetrator: Who's committed fraud

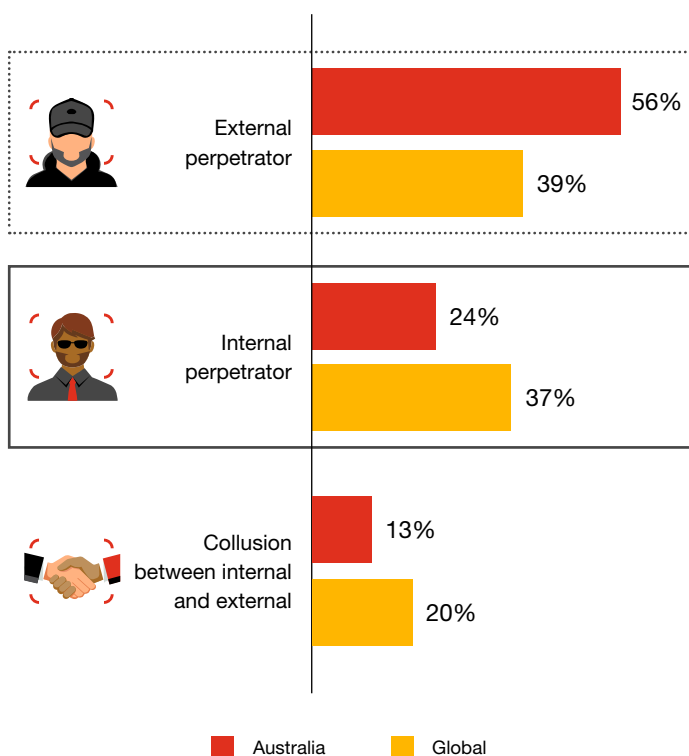
Internal or external?

Some frauds – such as external frauds – are transactional in nature, and lend themselves to active monitoring and potentially more limited financial impact. For other frauds like bribery & corruption or those internally perpetrated, it's about managing and mitigating the downside risk. These frauds tend to be harder to predict and monitor, often result in more costly fines, and have knock-on effects such as lost business, brand harm, and/or legal action from third-parties affected by them. These findings are telling at a time where there is greater scrutiny of organisations, and higher standards expected from consumers and shareholders in the wake of the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry and other recent regulatory events.

Among Australian respondents who had suffered fraud incidents in the past two years, 56% said these incidents were external compared to 24% internal. This is in striking contrast to the global findings, where incidents of the two types of fraud were in almost equal balance – with 39% being committed by external perpetrators, and 37% by people inside the business.



Perpetrators: External, internal and collusion between them



Source: PwC Global Economic Crime and Fraud Survey 2020

Customer fraud is on the rise

A form of external fraud that's growing especially strongly at a global level is customer fraud. For organisations globally, fraud committed against them by their customers tops not only the list of external perpetrators (at 26%) for the most disruptive frauds, but also the list of all frauds experienced (at 35%). Not surprisingly, customer fraud is especially prominent in the financial services and consumer segments – a correlation that could become more telling, as a growing number of industries shift to direct-to-consumer strategies.

Zeroing in on the survey responses from Australian companies, we find that Australia is actually running ahead of other countries in terms of the rise of customer fraud. 44% of Australian respondents who had suffered an incident indicated that they had been impacted by customer fraud in the past 24 months, well above the global figure of 35%.

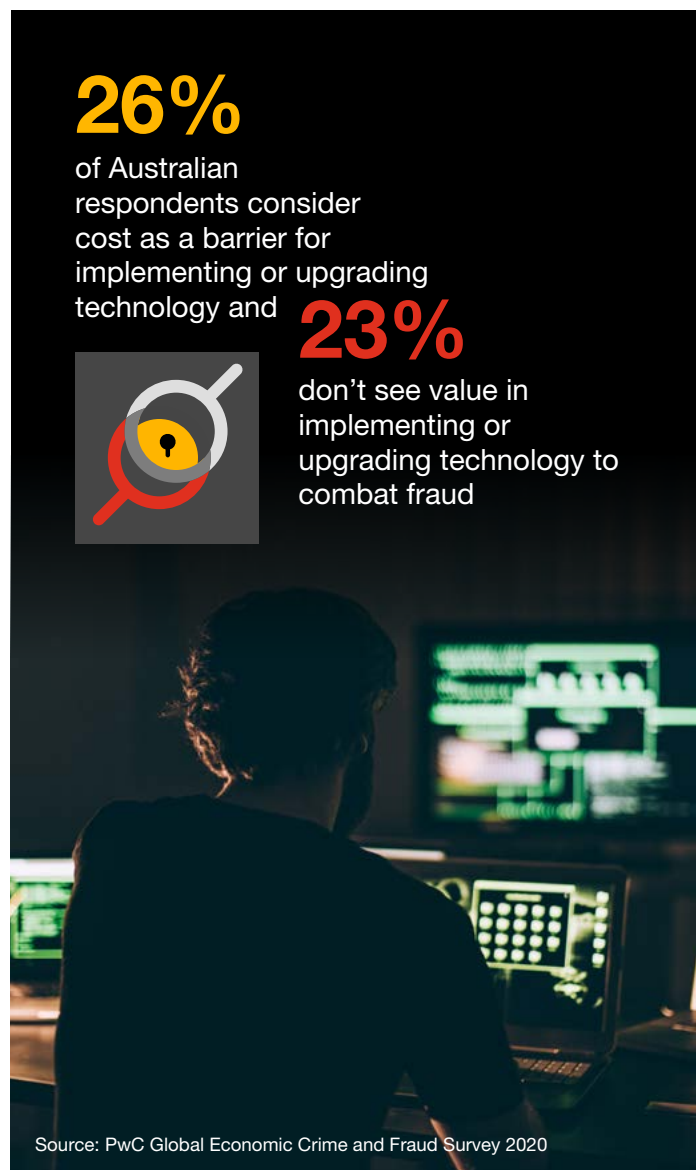
Australian companies also find customer fraud more disruptive than organisations elsewhere: one in five Australian respondents said customer fraud was the most disruptive/serious type of economic fraud they had encountered during the two years, five percentage points higher than the global figure. Together, these findings suggest that customer fraud is a threat that Australian companies should pay particular attention to.



Feeling the impact: **Positive outcomes and challenges**

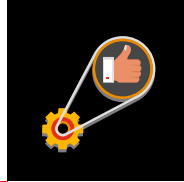
Responses to fraud

As well as highlighting these gaps in fraud prevention programs, our findings also underline the value of being able to respond effectively to a fraud once it's happened, and apply the lessons learned to good effect. When organisations have been impacted by fraud, many find they are able to use the incident as a significant driver of positive change across the business. Of the Australian respondents who had been impacted by fraud in the past two years, some 60% said the experience had helped them to streamline their operations, 50% to embrace new technology, and 43% to ensure incidents were reduced subsequently.



Barriers to new anti-fraud technologies

Less positively, when it comes to implementing or upgrading technology to combat fraud, Australian companies still find it more difficult than those elsewhere to make the business case for such investments. When asked what factors were preventing them from implementing technology to prevent fraud, over one in four (26%) of our Australian respondents identified cost as the biggest barrier into implementing it - in line with 27% globally. The resulting relatively low level of investment in anti-fraud measures, programs and technology emerges repeatedly in our research.

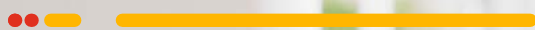


Feeling the impact: The costs of fraud

Turning to the costs of frauds, globally the average financial impact of each incident is trending upwards, with 22% of respondents globally reporting a cost of above US\$5 million (AU\$7.1 million) resulting from fraud in the past two years, and 36% saying they had lost more than US\$1 million (AU\$1.4 million).

The cost profile in Australia is similar, with 22% of Australian companies reporting they had lost more than US\$5 million (AU\$7.1 million) due to fraud, and 40% saying it had cost them more than US\$1 million (AU\$1.4 million). These financial impacts are substantial – reinforcing the need to double-down on efforts to detect and address fraud.

22%
of Australian
organisations **lost over**
AU\$7.1m
and an additional
40% over **AU\$1.4m**
in the last 24 months
due to **fraud**



Source: PwC Global Economic Crime and Fraud Survey 2020

Key themes

Looking across this year's findings from our Australian respondents, a number of themes emerge. **The most prominent include the quality and sophistication of companies'**

•• fraud detection capabilities – including the extent to which this is enabled by technology; the approach to remediation after a fraud; cybercrime, which is a more prevalent issue in Australia than elsewhere in the world; the fraud risks posed by third-parties, including suppliers; and then effectiveness of the response when a fraud happens.





Detection capability: Opportunities to use technology

While technology is just one part of an effective fraud detection capability – the right resources and expertise are also vital – it's undeniably an important one. Our research suggests Australian companies are still lagging behind the rest of the world in embracing technology to combat fraud.

58%

of Australian respondents agreed '**strongly**' or '**slightly**' that their organisation had been able to **implement or upgrade relevant technologies** in the past two years, against a global figure of 67%







Source: PwC Global Economic Crime and Fraud Survey 2020

A similar technology implementation gap emerges when we ask companies about the extent to which they're leveraging Artificial Intelligence (AI) and other disruptive technologies in their anti-fraud programs. The proportion of Australian companies with no plans to use AI is higher than the global average across all forms of AI, including machine learning and biometric authentication. There's a clear opportunity for companies in Australia to differentiate and elevate their anti-fraud capabilities to a new level by increasing their use of AI.

A roadmap for better fraud detection

Overall, for Australian companies looking to put robust fraud detection and prevention measures in place, we would advocate the three steps highlighted in the following information panel (p.9). Our research shows that nearly two-thirds of companies worldwide have policies and procedures in place to mitigate fraud risk, with the majority of these (6 in 10) including training and monitoring. Yet barely half of organisations are dedicating resources to risk assessment, governance, and third-party management. As our three-step approach underlines, these gaps need to be filled – with the support of the right technology.

More Australian respondents than global respondents **do not plan** to use any form of Artificial Intelligence.

Form of AI	Global	Aus
 Natural Language Processing	35%	49%
 Natural Language Generation	36%	49%
 Voice Recognition	36%	43%
 Machine Learning	31%	45%
 Biometric Authentication	30%	44%
 Other AI	21%	48%

Source: PwC Global Economic Crime and Fraud Survey 2020

Three steps to an effective fraud detection and prevention program



1 Identify all your risks and address on a prioritised basis

Companies can perform robust risk assessments, gathering internal input from stakeholders across the organisation and across geographies, to identify risks and assess mitigating factors. These assessments should also incorporate external elements. There is a wealth of information available in the public domain, and ignoring it could potentially result in a big miss. Risks should be assessed at regular intervals – not via a “once-and-done” approach.



2 Back-up your technology with the right governance, expertise, and monitoring

Recognise that one tool won't address all frauds and technology alone won't keep you protected. Technology often is only as good as the expert resources and regular monitoring dedicated to it.



3 Escalate, triage and respond

The ability to react to a fraud once identified is an important capability and element of an effective fraud program. The ability to quickly mobilise the right combination of people, processes and technology can limit the potential damage. In some cases, a disruptive fraud may be an opportunity – or a strategic inflection point – to trigger broader organisational transformation for brand protection.



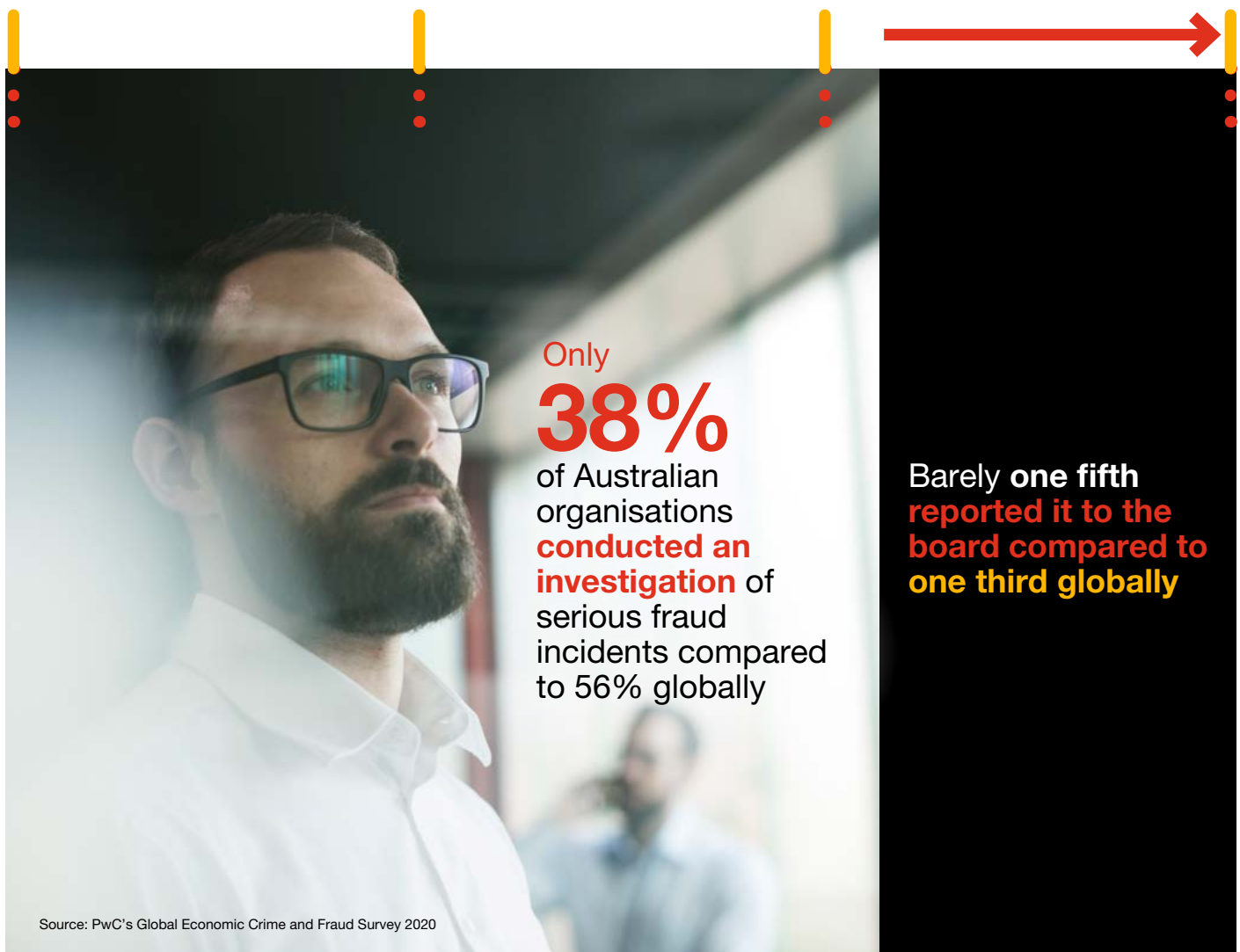


Remediation: **Do more, spend less**

When a fraud incident occurs our global research indicates that well over half – 56% – of organisations worldwide respond by conducting an investigation into why it happened and what lessons can be learned. What's more, nearly 60% of companies who had conducted an investigation said they ended up in a better place afterwards.

In Australia, just 38% of the organisations hit by a fraud said they had conducted a post-incident investigation – meaning they're missing out on the opportunities to learn from the experience.

Also, when Australian companies do conduct an investigation into a fraud, they tend to spend more on it than the average global respondent. This points to an opportunity to be more effective and efficient in response and remediation activities. For example, in terms of the response to an incident, 14% globally said they spent more than US\$1 million (AU\$1.4 million), compared to 23% of Australian organisations. On remediation, 18% globally spent more than US\$1 million (AU\$1.4 million), compared to 28% in Australia. And in terms of resulting fines and penalties, 19% globally reported costs of more than US\$1 million (AU\$1.4 million), against 23% in Australia.

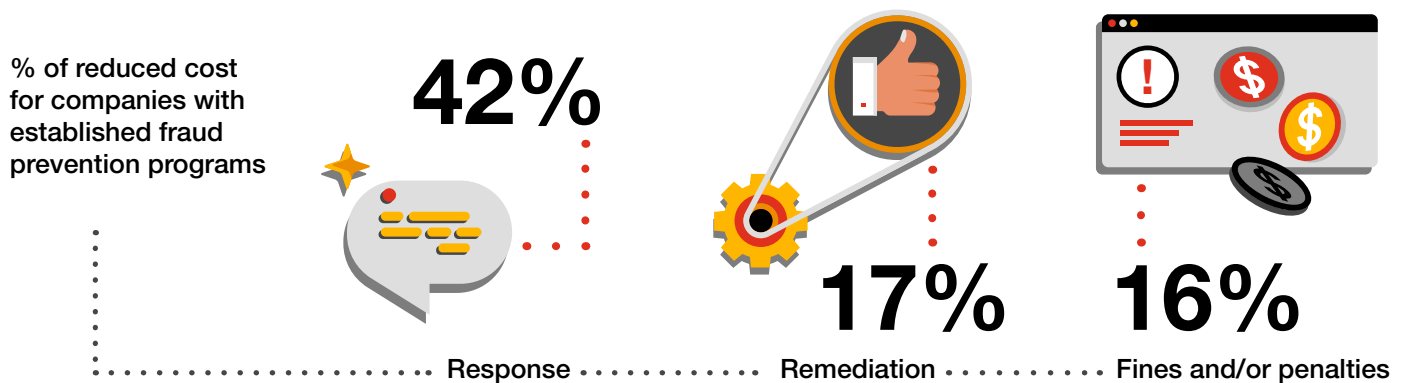




Remediation: Do more, spend less



Companies who invested in fraud prevention incurred lower costs when a fraud was experienced



Source: PwC's Global Economic Crime and Fraud Survey 2020

The last of these findings underlines the increasing attention that regulators – not least in Australia – are paying to companies' compliance programs, with many now starting to demand that companies provide evidence showing their compliance programs are effective. Equally significant, our global research shows that companies with dedicated fraud programs generally spent less overall (relative to revenue) across response, remediation and fines than those without. So, there's a clear link between fraud prevention investments made up front and reduced cost when a fraud strikes.



Tackling cybercrime: **Greater vigilance, more communication**

A higher proportion of Australian respondents (49%) have experienced cybercrime over the past 24 months than the average for respondents globally (34%). However, it's not all doom and gloom. The figure for global respondents has remained relatively consistent over the past six years, having stood at 33% in 2016 and 31% in 2018. By contrast, the figure for Australian respondents has declined during the same period, falling from 65% in 2016 to 43% in 2018 before rebounding this year.

That said, given that it seems Australian organisations are being particularly targeted by cyber criminals, there is still much more to do. Our study points to opportunities for Australian respondents to improve a number of elements of their cyber fraud programs – with two in particular coming to the fore.

The first is training and communication: just 11% of respondents globally do not have training or communications related to cybercrime risks, compared to 26% of Australian organisations. The second is mitigating the scale of its disruptive impacts: almost one-third – 32% – of Australian respondents cited cybercrime as the most disruptive/serious type of fraud in terms of the impact on their organisation (whether monetary or otherwise), compared to just 16% globally.

49%

of Australian respondents who reported **experiencing fraud** in the last 24 months reported **experiencing cybercrime**, higher than the global response of **34%**

32%

of Australian respondents felt that cybercrime was the **most disruptive/serious** in terms of **impact** to their organisation (monetary or otherwise) compared to **16% of global respondents**

Source: PwC's Global Economic Crime and Fraud Survey 2020



Third-party risks: Improving due diligence



66%

of Australian respondents do not have **mature, documented, risk-based due diligence** and ongoing **monitoring processes** in place for third-parties their organisations partner with

Source: PwC's Global Economic Crime and Fraud Survey 2020

As we highlighted earlier, 56% of Australian respondents who had suffered a fraud incident in the past 24 months indicated that the perpetrator was external, compared to just 39% of organisations globally. This appears to reflect the fact that the opportunities for third-parties to commit fraud have increased in recent years, as more Australian companies have decided to outsource non-core competencies to contain costs.

While these business partnerships can be valuable, they can be fraught with fraud risk – a threat that many companies in Australia and beyond have not formally addressed. In our global study, one in five respondents cited vendors and suppliers as the source of their most disruptive external fraud. But despite growing awareness of the potential threat from third-parties, 21% of companies globally said they had no third-party due diligence or monitoring program at all.

This lack of appropriate due diligence is also an issue in Australia: some 66% of our Australian respondents told us they do not have mature, documented, risk-based due diligence and ongoing monitoring processes in place for third-parties they partner with. So Australian companies have scope to reduce their fraud risks significantly by improving their fraud prevention programs in relation to third-parties.



When crisis strikes: **Responding with the right moves**

A further area of opportunity that emerges from our research is the potential for Australian companies to raise their game in responding to incidents. A comparison between the findings from our Australian and global respondents reveals that organisations in Australia are relatively poorly prepared to handle incident response across a whole range of factors. These include:

Teamwork
40%

of Australian respondents **strongly agreed that they acted as a team**, compared to 47% of Global respondents.

Data access
32%

of Australian respondents were **able to access the data required for incident response**, compared to 39% of Global respondents.

Communication
33%

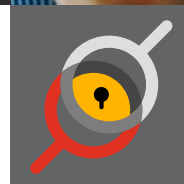
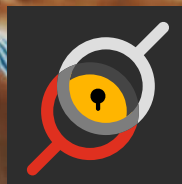
of Australian respondents **believed they communicated effectively**, compared to 41% of global respondents.

Source: PwC's Global Economic Crime and Fraud Survey 2020

As these findings underline, there's a clear need for Australian companies to improve their incident response processes and capabilities – or risk facing greater damage from incidences of fraud than their counterparts elsewhere.



Conclusion



Time to zero in on fraud risks

Both the Australian and global findings from our latest Global Economic Crime and Fraud Survey underline one stark fact: that fraud risks are a constant reality for all businesses in every geography – and that being well-prepared to detect, manage and respond to them is a prerequisite for any sustainable and well-managed organisation.

From an Australian perspective, our findings suggest that organisations elsewhere in the world are actually being confronted by more fraud incidents than those based in Australia. But this finding is **offset by what seems to be a lower degree of rigour and technology enablement in Australian fraud detection processes**, and less well-developed incident response capabilities.

Considering the challenges posed by the COVID-19 pandemic, these shortcomings are exposing Australian businesses to risks that are essentially unquantifiable.

Even if you have an effective anti-fraud program in place, it's vital that you continue to assess and refine it. And the need for continual improvement is ever more pressing as organisations grapple with economic downturn and endeavour to accelerate digitisation plans to adapt to new ways of working and interacting with customers.

So, what should you do? The answer comes back to the steps mapped out. In short, get a clear view of all your fraud risks; implement the right combination of technology, governance and expertise to address them; and be committed to moving decisively when a fraud strikes.

The message is clear. Your business should dedicate effort and resources to getting a firm grip on your fraud exposures as a matter of priority. When a fraud hits, it's an investment that will pay for itself many times over.

To learn more

Better understand your economic crime and fraud risks and assess your programs against your peers and our global respondents.



Mark Rigby

Sydney
PwC Australia
mark.rigby@pwc.com
+61 403 823 157



Penny Dunn

Melbourne
PwC Australia
penny.dunn@pwc.com
+61 407 367 561



Simon Taylor

Melbourne
PwC Australia
simon.c.taylor@pwc.com
+61 409 252 465



© 2020 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which 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.

127077334