Fraud out of the shadows

New Zealand insights from PwC's Global Economic Crime Survey 2018

51%

of NZ organisations have experienced economic crime in the past two years

42%

of NZ organisations felt that cybercrime would be the most disruptive crime over the next two years

58%

of NZ organisations consider that opportunity was the main driver of economic crime

pwc

pwc.co.nz/crimesurvey2018

Stephen Drain
Partner
Forensic Services
PwC New Zealand

Welcome to the 2018 PwC Global Economic Crime Survey

The PwC Global Economic Crime Survey is the largest survey of its type. With over 7,200 respondents this year, it collects a wealth of information on the trends and impacts of economic crime.

This year's findings tell us that the economic crime picture in New Zealand is changing, as it has in the past. Increasingly boards and management are challenged to know how to respond to economic crime; both the threat of it and when an event occurs. Planning with a focus on prevention and detection can go a long way to mitigating the risks and in the process create a transparent and safe environment for employees, clients and stakeholders.

Managing economic crime need not just be a cost. If properly addressed, a strong fraud control framework can create a competitive advantage for businesses in an increasingly diverse and complex borderless environment.

I hope you will get some value from our insights this year and look forward to the opportunity to discuss it with you. Please feel free to contact me, my team or your local PwC contact to discuss the survey further.

Fighting fraud

Executive Summary

Organisations today face a perfect storm of fraud risk – internal and external threats, with regulatory and reputational risks – in an era of unparalleled public and regulatory scrutiny.

51% of New Zealand organisations report that they have been the victim of economic crime in the past 24 months. At first glance this figure seems high.

Aren't we a reasonably honest lot in New Zealand? Don't we have a trusting environment in our workplaces? These things are true, but perpetrators of economic crime have always been amongst us, and this key New Zealand statistic is consistent with global experience. We are not alone in experiencing economic crime and its impacts.

Economic crime can be seen as a costly nuisance, to be dealt with using ad-hoc, or stopgap measures. However, given the widespread nature of the problem, and in the wake of large-scale corporate scandals and new standards for public accountability, fighting economic crime has progressed from an operational or legal matter to a central business issue.

Insights on current New Zealand and global findings bring the picture to life to enable your organisation to draw on global and local experience – whether that be sector, type of risk or the latest findings on the drivers for fraudsters.

This year's respondents record that, in New Zealand:

- Just over half experienced economic crime in the past 24 months;
- Cybercrime continues to increase and is expected to cause the most disruption to businesses going forward;
- Establishing an appropriate culture is imperative to fighting economic crime and organisations continue to be reliant on whistleblowers to a large degree; and
- Financial institutions are still finding anti-money laundering compliance a challenge. This year, new legislation brings lawyers and accountants into the regime.

Our study also shows that while there is growing awareness of the perils of economic crime, too few organisations are fully cognisant of the individual risk landscape they face. Understanding your risks, and establishing a fraud control framework that is meaningful for your organisation is key. Our report has cameos on discrete areas of focus as part of a wider inter-linked fraud framework.

With that in mind, we focus our insights on:

- The New Zealand landscape;
- Managing economic crime dynamically;
- The cyber threat; and
- Anti-money laundering.

The New Zealand fraud landscape

26%

of economic crimes saw the victims lose between **US$100,000 and US$1M**

Economic crime – the big picture

Economic crime today is tech-enabled, innovative, opportunistic and pervasive, and might be the biggest threat you don't know you have. Reported incidents experienced by New Zealand businesses have increased since our 2016 survey, from 40% to 51%.

Our survey reveals that New Zealand organisations are spending more than ever to fight economic crime, with 41% of respondents increasing their financial commitment to combating it over the past two years. 54% of the same group of respondents plan to boost their spending over the next 24 months.

Organisations are making more use of powerful technology and data analytical tools, many have expanded their whistleblower programmes, and most are keeping leadership in the loop. 90% of respondents reported that they had brought the most disruptive economic crime to the attention of either the board or senior leaders.

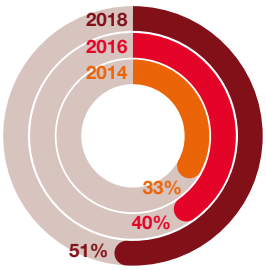
With over half of organisations reporting that they experienced economic crime it is clear that it deserves our attention.

As economic crime evolves, so has our study. Here are some of the enhancements we've made to this year's Global Economic Crime Survey:

- We've tweaked our definitions to make them crisper, breaking out both the defined types of fraud and cybercrime (refer to pwc.co.nz/crimesurvey2018).
- We've added questions on the specific types of technology organisations now use, with additional questions on their effectiveness.
- We've included valuable benchmarks on both the costs of economic crime and the amount companies spent on fighting it.

The impact of economic crime on industry sectors in the past two years

Source: PwC's 2018 Global Economic Crime Survey – Global respondents



51% of organisations report they have experienced economic crime – this continues to rise.

Source: PwC's 2018 Global Economic Crime Survey – New Zealand respondents

What type of economic crime are we experiencing?

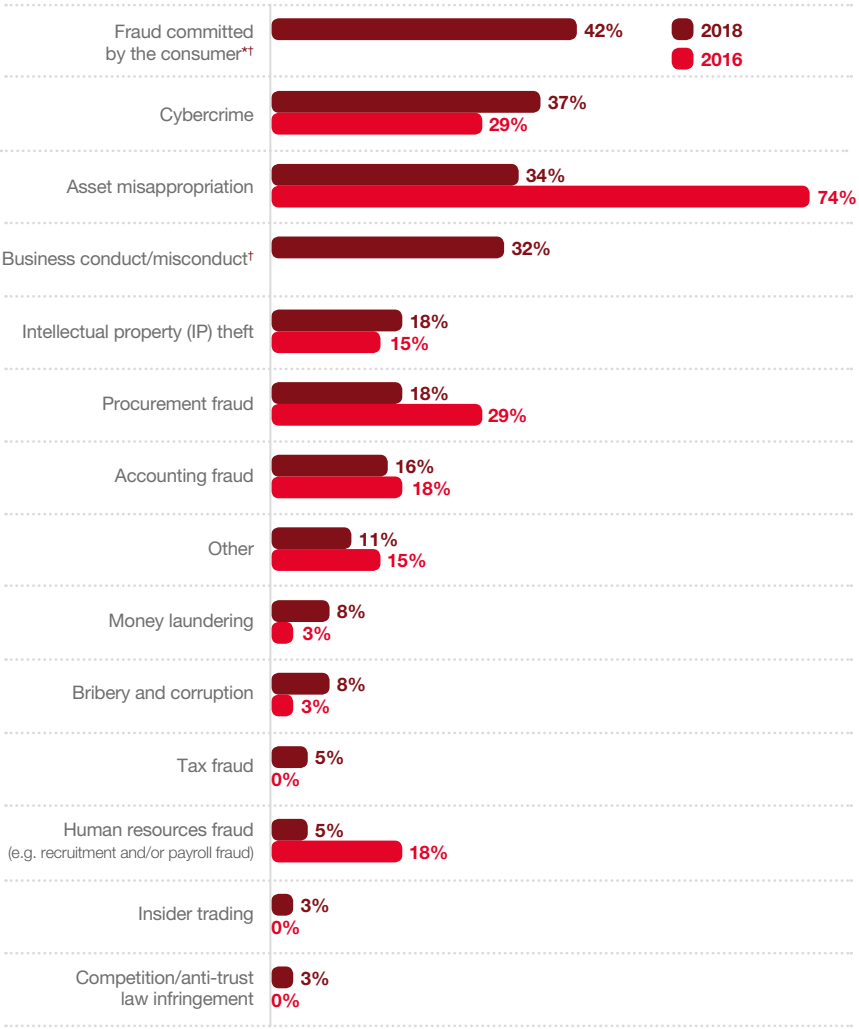
With the introduction of a new catergory; *fraud committed by the consumer*, asset misappropriation is no longer the highest reported type of economic crime affecting New Zealand organisations. 42% of New Zealand organisations reported experiencing this crime in the past 24 months, compared with a global average of 29%.

Cybercrime remains the second highest reported crime in our survey, and is the crime that respondents believe will be the most disruptive to their organisations over the next 24 months.

42% of respondents anticipate that cybercrime will be the most disruptive economic crime for their organisation in the next 24 months

Source: PwC's 2018 Global Economic Crime Survey – New Zealand respondents

What type of economic crime has your organisation experienced domestically within the last 24 months?

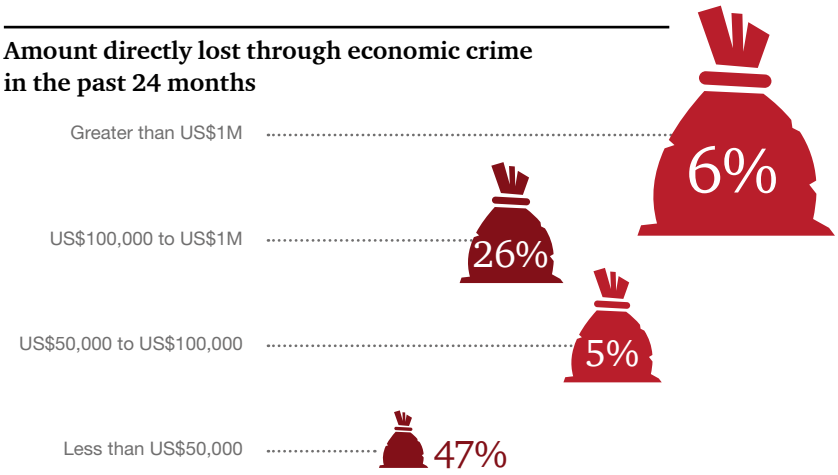


* Including mortgage fraud, credit card fraud, claims fraud, cheque fraud, synthetic ID.
† Fraud committed by the consumer and business conduct/misconduct are included for the first time in 2018.

Source: PwC's 2018 Global Economic Crime Survey – New Zealand respondents

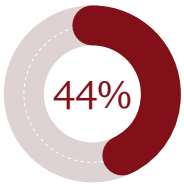
Cost of economic crime

Amount directly lost through economic crime in the past 24 months

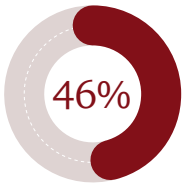


Source: PwC's 2018 Global Economic Crime Survey – New Zealand respondents

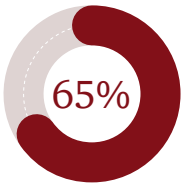
The other costs of economic crime



43% said that economic crime had an impact on **business relations**



46% said economic crime had an impact on their **reputation and brand**



65% said economic crime had an impact on **employee morale**

Source: PwC's 2018 Global Economic Crime Survey – New Zealand respondents

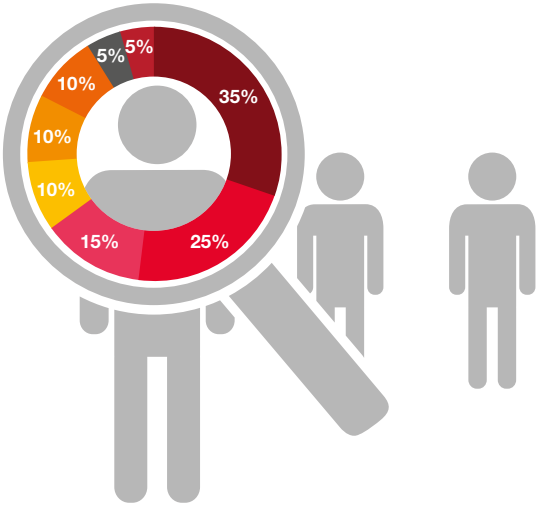
Who are the perpetrators?

When the perpetrator was an internal actor, 58% of respondents considered that the opportunities presented to them was the main driver in leading them to commit the crime. Opportunities include weak internal controls, including those which a manager (comprising 75% of internal offenders) might have the ability to override.

Where the fraudster was external to the respondent's organisation, a sizable percentage of that 'external' group were so-called 'frenemies': third parties – agents, vendors, and shared service providers – and customers. People and entities with whom organisations voluntarily interact, and from which one would expect a degree of mutual trust.

Although internal actors are a significant threat to New Zealand organisations at 36%, external actors are currently posing a bigger risk at 61%.

Who were the perpertrators of external economic crime against your organisation?



- **35%** Customer
- **25%** Hacker
- **15%** Other
- **10%** Agent/intermediary
- **10%** Vendor
- **10%** Don't know
- **5%** Consultant/advisor
- **5%** Organised crime

Source: PwC's 2018 Global Economic Crime Survey – New Zealand respondents

Integrity due diligence

Respondents to our survey record that, in the past 24 months, 25% of the external perpetrators of economic crimes have been their own third parties. 10% of these crimes were perpetrated by the business' agent or intermediary, 10% of cases were perpetrated by vendors, while the remaining 5% of cases were perpetrated by the business' own consultants, advisors or service providers. In an increasingly global marketplace, businesses need third parties in order to survive. However, every opportunity these relationships present, comes hand in hand with an element of risk; one that businesses must understand, mitigate and manage.

That's not all. The risk of crime perpetrated directly against their own organisation is only one of the concerns.

With increasing public scrutiny and regulation, a third party engaging in inappropriate behaviour can have devastating consequences for an organisation. For example, a third party with a director participating in anti-competitive behaviour, can lead to the loss of shareholder confidence, reputational damage, regulatory breaches or legal consequences for it and, importantly, its business associates.

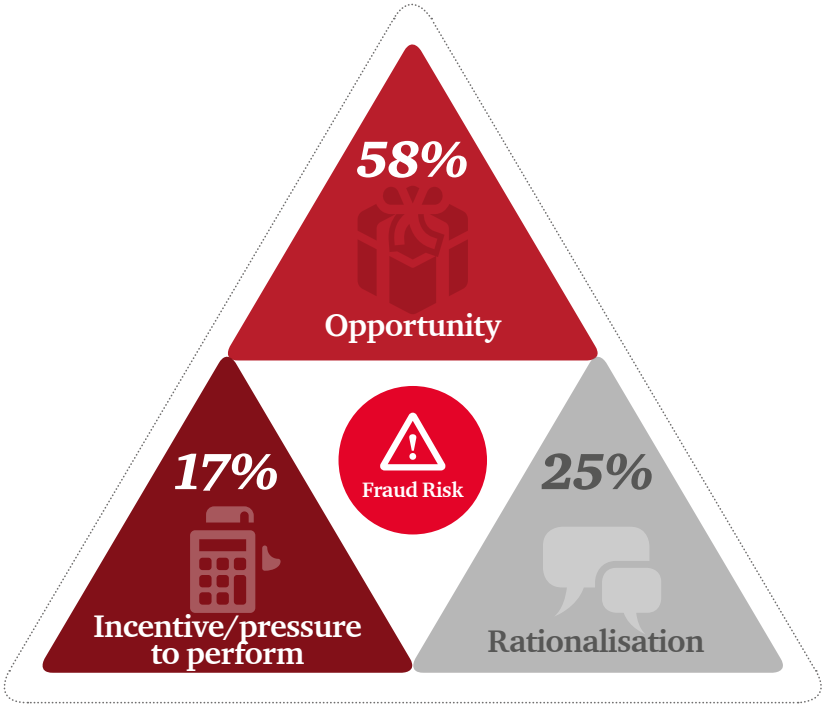
Bribery and corruption is also a very real risk when doing business with third parties. The New Zealand Ministry of Justice reports that there is compelling evidence that third parties are frequently used to conceal bribe payments. Not only that, but there are circumstances in which an organisation may be held liable for a bribe paid by one of its third parties, even when the organisation hasn't instructed the third party to do so.

An effective way to mitigate and manage this risk is to conduct integrity due diligence before entering into a relationship with a third party. This approach is not only recommended by the Ministry of Justice, but also by guidance accompanying anti-bribery and corruption legislation in the USA and UK, the remit of which may also extend to New Zealand businesses operating within those territories.

Gaining an understanding of a third party's experience and reputation assists in identifying 'red flags' of which any business partner should be aware. Identifying these will allow you to make an informed decision about the future of the business relationship.

The volume of publicly available information is at an all-time high, and continues to increase daily. Conducting integrity due diligence on potential new third parties should be a priority for New Zealand businesses going forward.

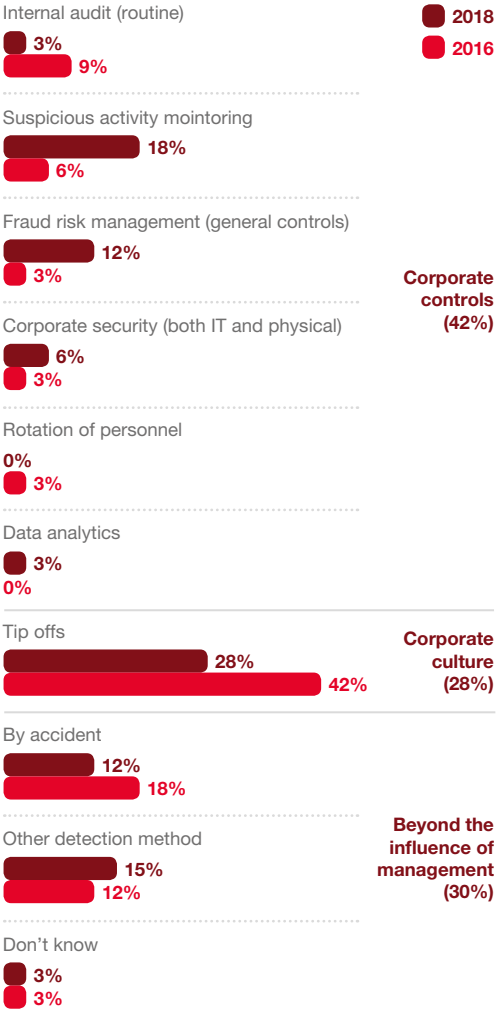
The fraud triangle: what makes an employee commit fraud?



Source: PwC's 2018 Global Economic Crime Survey – New Zealand respondents

Detection methods

How was the most disruptive economic crime detected?



Source: PwC's 2018 Global Economic Crime Survey – New Zealand respondents

Blind spots

Every organisation is vulnerable to 'blind spots' – the awareness or responsibility gaps that challenge even the best-run companies. By throwing light on those 'blind spots', you will find opportunities to take preventive action and make significant improvements in your efforts to fight economic crime. We discuss this further in this study.

Managing economic crime dynamically

As businesses, and the world in which they operate, change, the economic crime risks to which they are exposed change too. In today's rapidly changing world, it is imperative that businesses are responsive and flexible, and take a dynamic approach to identifying, mitigating and managing these risks to ensure that they aren't left exposed.

Who is responsible?

If you brought your senior leadership team together and asked them what they perceive their and each other's role to be in fighting economic crime, it is likely that you would hear many different answers. That's a problem, because it is in the gaps between what you are told – the blind spots, the overlaps, the places that are "not my responsibility" – that the greatest fraud risk lies. These gaps can have a significant, detrimental impact on the overall effectiveness of your fraud prevention efforts, financial performance, and regulatory outcomes.

20% of global organisations have adopted a centralised and dedicated fraud detection and investigation team, perhaps to combat this lack of clarity. This is compared to 8% of New Zealand organisations.

A centralised response can 'de-silo' functions like compliance, ethics, risk management and legal, and reduce the number of responsibility gaps and overlaps, enabling a more co-ordinated, proactive approach to economic crime.

However, an enterprise-wide fraud function can create a false sense of security amongst the employees on whom you rely to implement controls, and to identify and escalate their concerns. It is important that everyone understands both the big picture of fraud risk management and how their own function fits into that puzzle.

Identify your risks

The nature of your risks drives all other risk management activities. Yet only 52% of respondents reported that they have conducted a fraud risk assessment in the past two years.

Fraud risk assessments can be conducted internally, or by engaging outside expertise. They can take a holistic view of the business or be a 'deep dive' into a particular process which offers the biggest opportunity to perpetrators. Either way fraud risk assessments are best if reviewed regularly to ensure that they take into account the ever changing tools and techniques perpetrators use.

Fraud Control Frameworks (FCF) and risk assessments: A look at prevention

Having strong policies, procedures and controls are critical to making sure you have the institutional knowledge to prevent a fraud event, however it is often the unseen, or generally accepted aspects of an organisation, which create an environment susceptible to economic crime. A strong tone from the top, good staff awareness of managements approach to fraud, training and vetting of staff, a well-promoted whistleblower regime and strong ethical culture all assist in the prevention of economic crime. When these elements of FCF are present and complemented with a considered fraud risk assessment, organisations are typically well on the way to preventing economic crime. What steps is your organisation taking to prevent fraud? are you more willing to invest in detection of fraud rather than preventing it? All of this is part of your FCF.

So what are New Zealand organisations currently doing to prepare?

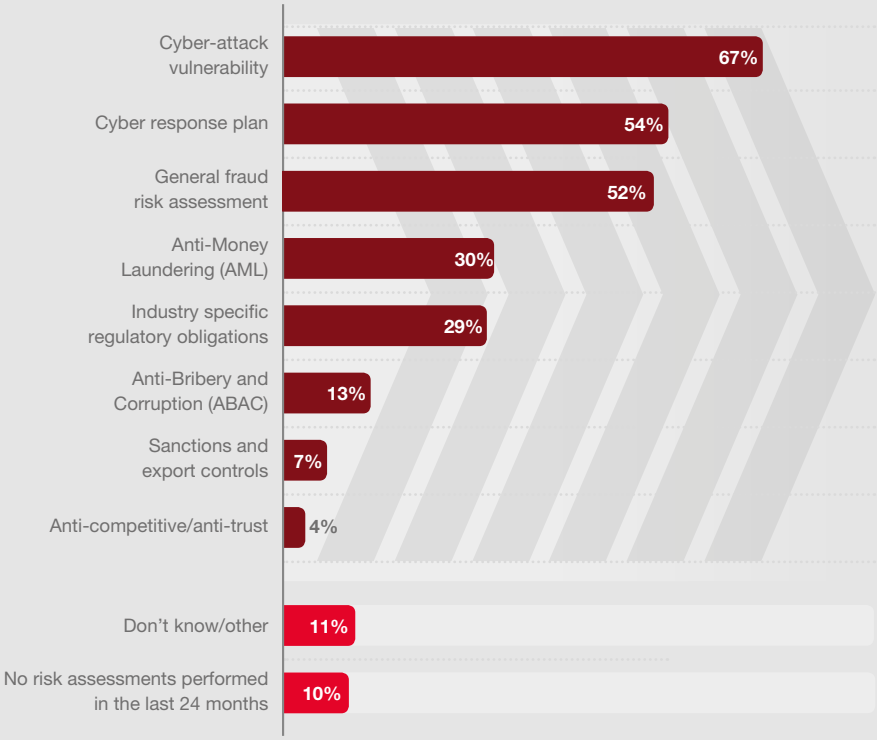
90% of New Zealand respondents are taking steps to identify the risks they face. However, when looking at fraud risks specifically, 52% of New Zealand organisations have performed a general fraud risk assessment in the last 24 months, meaning almost half of New Zealand organisations are not formally identifying the fraud risks they face. In the absence of performing a fraud risk assessment, organisations are not able to implement appropriate controls to mitigate these risks.

A fraud risk assessment to identify the specific risks your organisation faces, and a review of your organisation's FCF, will identify where you are vulnerable to fraud or economic crime.

We have recently seen organisations have a renewed focus on having a fit for purpose FCF, often done with the backdrop of recent victims of economic crime.

Only 20% of all respondents (who had been the victim of an economic crime) had performed a general fraud or other risk assessment as a result of a specific event. Given 51% of New Zealand organisations experienced economic crime, the majority of those who have suffered an economic crime did not re-examine their fraud risks. The risk here is that by focussing on known vulnerabilities from past events, organisations risk leaving themselves just as exposed as they were before.

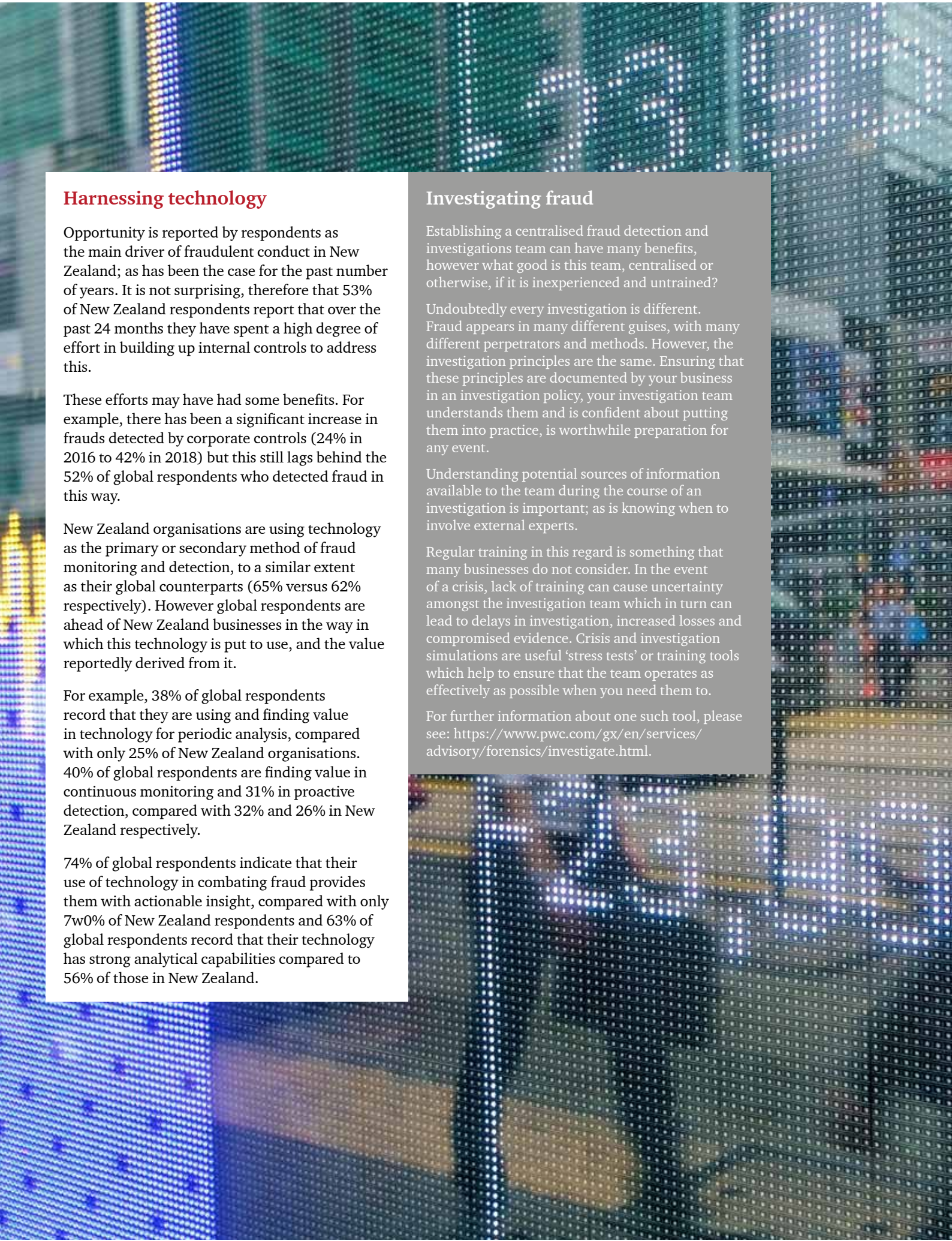
What risk assessments have you performed in the last 24 months?



Source: PwC's 2018 Global Economic Crime Survey – New Zealand respondents

What prompted your organisation to perform the risk assessment?

Source: PwC's 2018 Global Economic Crime Survey – New Zealand respondents



Harnessing technology

Opportunity is reported by respondents as the main driver of fraudulent conduct in New Zealand; as has been the case for the past number of years. It is not surprising, therefore that 53% of New Zealand respondents report that over the past 24 months they have spent a high degree of effort in building up internal controls to address this.

These efforts may have had some benefits. For example, there has been a significant increase in frauds detected by corporate controls (24% in 2016 to 42% in 2018) but this still lags behind the 52% of global respondents who detected fraud in this way.

New Zealand organisations are using technology as the primary or secondary method of fraud monitoring and detection, to a similar extent as their global counterparts (65% versus 62% respectively). However global respondents are ahead of New Zealand businesses in the way in which this technology is put to use, and the value reportedly derived from it.

For example, 38% of global respondents record that they are using and finding value in technology for periodic analysis, compared with only 25% of New Zealand organisations. 40% of global respondents are finding value in continuous monitoring and 31% in proactive detection, compared with 32% and 26% in New Zealand respectively.

74% of global respondents indicate that their use of technology in combating fraud provides them with actionable insight, compared with only 7w0% of New Zealand respondents and 63% of global respondents record that their technology has strong analytical capabilities compared to 56% of those in New Zealand.

Investigating fraud

Establishing a centralised fraud detection and investigations team can have many benefits, however what good is this team, centralised or otherwise, if it is inexperienced and untrained?

Undoubtedly every investigation is different. Fraud appears in many different guises, with many different perpetrators and methods. However, the investigation principles are the same. Ensuring that these principles are documented by your business in an investigation policy, your investigation team understands them and is confident about putting them into practice, is worthwhile preparation for any event.

Understanding potential sources of information available to the team during the course of an investigation is important; as is knowing when to involve external experts.

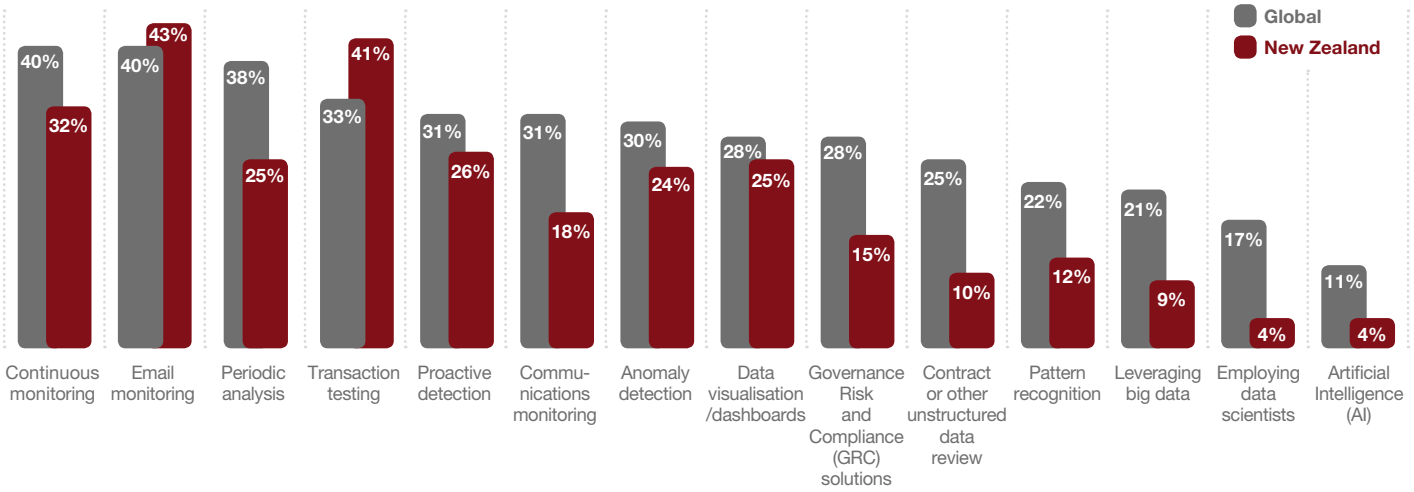
Regular training in this regard is something that many businesses do not consider. In the event of a crisis, lack of training can cause uncertainty amongst the investigation team which in turn can lead to delays in investigation, increased losses and compromised evidence. Crisis and investigation simulations are useful 'stress tests' or training tools which help to ensure that the team operates as effectively as possible when you need them to.

For further information about one such tool, please see: https://www.pwc.com/gx/en/services/advisory/forensics/investigate.html.

Organisations need to strike a balance between acting on fraud red flags, and being overzealous in sending alert communications to their customer. The margin for error is small. On the one hand, you run the risk of missing a fraudulent transaction (with the financial and reputational fallout that follows). On the other, you risk alienating your customer base: more than one in five respondents (21%) said they thought their organisation's use of technology to combat fraud and/or economic crime was producing too many positive alerts.

The business case for investment in fraud technology goes beyond protecting against reputational, regulatory or financial damage. It includes reducing the cost of fraud prevention through efficiencies and fine-tuning your fraud programme to reduce 'customer friction' – allowing your good customers to interact more freely with your platform and your product, without excessive fraud prevention controls getting in the way. There is scope for New Zealand organisations to do more to ensure they are using technology in this way.

Respondents deriving value from alternative and disruptive technologies in fighting fraud



Source: PwC's 2018 Global Economic Crime Survey – New Zealand respondents

Investing in your people

No matter how sophisticated an organisation's internal controls and monitoring programmes are, an individual intent on circumventing them will find a way to do so. Therefore, addressing internally committed fraud requires more than technology and processes; it requires a focus on the culture driving or enabling the misbehaviour.

This is an area in which New Zealand organisations have seen some progress. However, more can be done.

The number of frauds detected as a result of corporate culture (i.e. tip offs both internal and external) have decreased (from 42% in 2016 to 27% in 2018) and only 57% of New Zealand respondents say that they have a formal business ethics and compliance programme.

Organisations that fail to clearly define ethical conduct risk being unable to hold employees to account for what could be considered to be unacceptable behaviour.

You need a rule book to define the boundaries of acceptable behaviour.

Whistleblower essentials

Safe: Those that want to make a disclosure will need to feel that in doing so, they are not going to face any negative consequences. Genuine whistleblowers may also want legal protection. The Protected Disclosures Act 2000 prescribes that certain public and government entities must have policies and procedures in place for whistleblowers. Many of our clients are private commercial businesses who have effectively 'opted in' to the requirements of the Act meaning that their employees can make disclosures through PwC as an independent party, and be protected from any employment or other actions from having done so (assuming it's a genuine concern).

Mechanisms: One size doesn't fit all. Some employees will be happy to talk to their boss, or their boss' boss. Others will want to talk to someone in governance, or an external service, or not talk at all and instead send an email. A whistleblowing service should be part and parcel of a wider system for employees to disclose potential wrongdoing. No matter the procedures in place, or the level of communication and training implemented, we are often surprised at the differing paths whistleblowers take to make a disclosure.

No mention on whistleblowing would be complete without mentioning that there can be negative connotations when discussing whistleblowers: those that breach the rules (or laws) to reveal private information that has no public interest or could not be said to be a disclosure of wrongdoing. Employees or others minded to make those sorts of disclosures are unlikely to contact an independent service.

So we need not confuse the genuine concerns of employees with this behaviour. One of the key things that a responsible organisation can do to build trust in its whistleblower service is to ensure that genuine concerns raised through it are promptly and thoroughly investigated. Even if the matter appears trivial, or could more appropriately have been initiated through say an employee process, allowing such matters to be dealt with through the whistleblowing process builds trust in the service, so that when the worst happens, someone in the know will pick up the phone.

The cyber threat

How can you fight cybercrime more effectively?

The second most common economic crime in New Zealand was cybercrime[1]. It was suffered by 37% (up from 29% in 2016) of the respondents who had experienced an economic crime in the past two years. Cybercrime now tops the list in both the United States and the United Kingdom, and on current projections, also looks set to take over the top spot in the New Zealand survey.

Today's cybercriminals are equally, if not better resourced than the organisations they attack; therefore, a new perspective is required. While measurements of the occurrence and impact of cybercrime is useful, it is strategically more beneficial to focus on becoming better prepared to respond. However, our survey points to the troubling fact that New Zealand organisations remain unprepared to deal with a cyber-attack. A closer look at the figures reveals why.

During 2017, a significant number of organisations fell victim to a number of targeted, highly sophisticated and successful cyber-attack campaigns. The WannaCry and Petya ransomware attacks exploited a known vulnerability, which left untreated, could spread with little user interaction from a single computer through to the entire infrastructure. This had both a direct impact to those who were infected, along with collateral damage to a number of third parties (via email outages and the like).

It is therefore not surprising that 42% of New Zealand respondents felt that cybercrime would be the most disruptive crime they will face over the next two years, which is considerably higher than the global average of 26%. This is also significantly more disruptive than any other crimes in New Zealand, with asset misappropriation coming in second, at only 12%.

37%

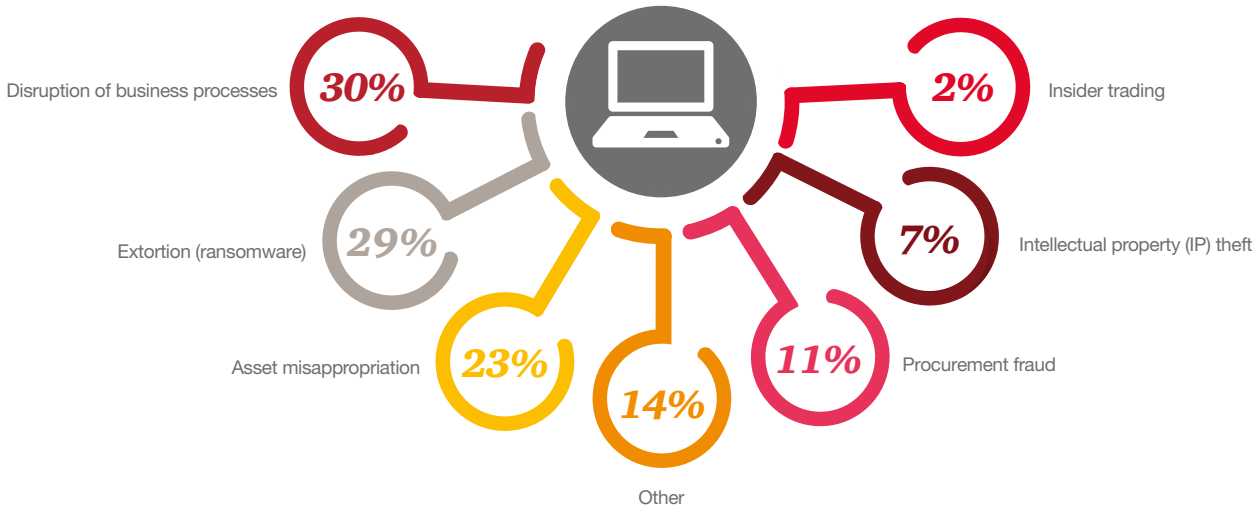
of economic crimes were cybercrime

[1] Cybercrime is any criminal offence committed using computer equipment, where the electronic device was the main element and not an incidental one. Typical instances of cybercrime include the theft of intellectual property or other assets by insiders and cyber-attacks by external parties.

By understanding the motivations and attack patterns of your enemy, you can improve your ability to defend. Such enemies include amongst others, insiders, nation states, organised crime groups and hacktivists. Our respondents were most concerned about external parties launching cyber-attacks[2], which target the availability, confidentiality or integrity of computer systems and data.

The most prevalent cyber-attacks in New Zealand were by far, phishing[3] and malware[4], which in turn resulted in significant disruption of business processes and digital extortion.

Types of fraud that organisations were a victim of through a cyber-attack



Source: PwC's 2018 Global Economic Crime Survey – New Zealand respondents

Electronic evidence in fraud investigations

While externally perpetrated cyber-attacks are on the rise, New Zealand organisations continue to fall victim to employee misconduct.

For example, an employee steals intellectual property. Data on computer systems, mobile devices and other network data will need to be forensically collected and examined using specialist tools to determine, to the extent possible, any evidence of wrongdoing.

These same forensic tools are also critical during litigation and regulatory enquiries. To meet the demands of today's volume and variety of data, specialised tools and processes are required to ensure that the processing, review and production of relevant documents are both completed in a timely and accurate manner. Technology assisted review techniques such as predictive coding can further reduce the time taken and improve accuracy.

[2] Cyber-attack is malicious activity e.g. a Distributed Denial of Service (DDOS) or a Ransomware attack.

[3] A phishing attack attempts to obtain confidential information including logins, passwords and financial details, often for malicious reasons. Attacks are launched via electronic communications, disguised to be from a trustworthy source.

[4] Any form of malicious software that infects your network, servers, devices, or end user computers, including Ransomware, remote access tools, network sniffing software, and botnet software.

So what are New Zealand organisations doing to respond to this threat?

People
The attacks of 2017 raised the profile of cybercrime in amongst New Zealand's decision makers, and fortunately, they are taking this threat seriously. In 2017, 44% of CEOs[5] were unsure about their ability to respond to a cyber-related crisis. In 2018, CEOs[6] cited cyber-attacks as posing the greatest threat to their growth targets, confirming that cyber is not just an issue which concerns the IT team. It is pleasing to see now that over half of our New Zealand respondents have an IT security manager or Chief Information Security Officer (CISO) reporting directly through to the executive.

Process
A cyber risk assessment is a good starting point. Over the last two years, 67% of our survey respondents made an effort to identify which of their critical assets were vulnerable to attack, and they responded accordingly to manage cyber security risk to systems and data.

New Zealand respondents also cited that Policy, Training, Multi-factor Authentication and Penetration Testing/Vulnerability Assessments were amongst the most common measures taken as part of their cyber security programmes.

In line with the global average, we are pleased to see that the percentage of respondents who have a fully operational cyber incident response plan has increased to 64% (from 45% in 2016), with a further 14% currently implementing their plans. The plan should be tested regularly via simulated table-top exercises to ensure that it is easy to follow for all participants, including the computer incident response team and any non-technical experts. Similarly, Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) should also remain current and effective.

Technology
Technology rapidly changes, so you should manage your evolving threat landscape through a tailored cyber security strategy and programme of work. A useful resource is the United States National Institute of Standards and Technology Cyber Security Framework (NIST CSF) which sets out the five critical functions of identify, protect, detect, respond and recover. For example, you may identify that your servers containing payroll data are critical. You would then protect this data from attack by determining any vulnerabilities to those servers and treating them. On detection of a breach, you would have well defined processes in place to return to business as usual. According to our 2018 Global State of Information Security Survey, traditional software vulnerabilities (e.g. out-of-date software, unpatched software) was the most common cause of a security incident. Accordingly, the WannaCry and Petya vulnerabilities resulted in a rush on software patching programs.

[5] The New Zealand CEO Survey 2017.

[6] The New Zealand CEO Survey 2018.

What are the most common types of cyber-attack in New Zealand?

Phishing

At 61%, phishing was the most common type of cyber-attack reported in New Zealand, which is nearly double the global average.

Phishing attacks have been commonplace since the mid 1990s, so why is phishing still so prevalent? For some time, technology has been effective at filtering out large volumes of suspicious emails. However, the sophistication of targeted attack campaigns (spear-phishing[8]) combined with basic human vulnerabilities has resulted in ongoing success by the attackers. They take advantage of our curiosity by enticing action, such as naming attachments "Executive_Salary_Details.xls". The shift to using the Cloud has also placed data beyond the traditional physical security perimeters of an organisation, whereby attackers can more readily access and copy the breached data.

The impact of a phishing attack may include a loss of access to email accounts, which are then used to launch further attacks, resulting in the blacklisting of the email domain. Other impacts include the loss of confidential information and damage to reputation, as well as causing immeasurable distress to the victim(s).

Malware

The second most common type of cyber-attack on New Zealand respondents was malware (49%). Our respondents also reported that ransomware was amongst the most pervasive type of malware.

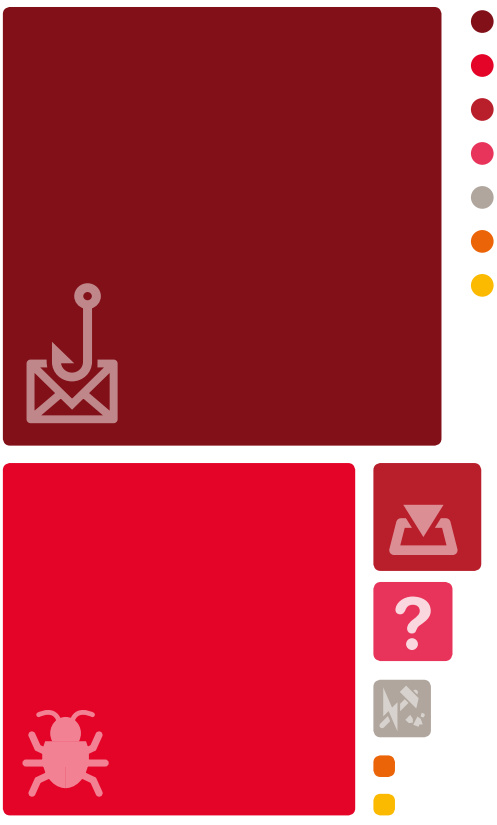
Ransomware has exploded in recent years, the effect of which prevents or limits user access to computer systems or files. The attackers typically demand a ransom payment (often using a cryptocurrency such as Bitcoin) in exchange for the key.

As Ransomware continuously evolves, its behaviour and distribution methods vary in many different ways. Organisations seeking to improve their cybercrime defences against a ransomware attack should plan for, and test, their level of preparedness. Initiatives can include:

- User training and awareness.
- Cyber incident response plans, setting out the balance between operational and forensic requirements.
- Cyber incident response table-top exercising.

One of the most effective ways to prevent a phishing attack is to train your staff as to how to spot a phishing email, report its existence and safely delete it.

Cyber threat: What are the most common types of attack in New Zealand?

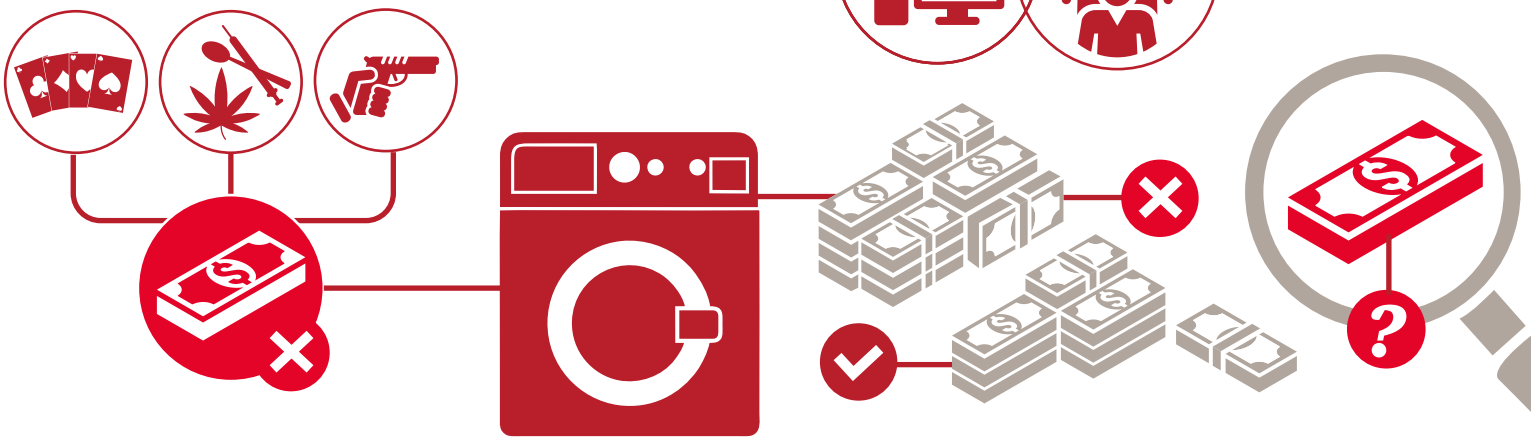


- 61% Phishing
- 49% Malware
- 15% Network scanning
- 11% Don't know
- 8% Brute force attack
- 4% Other technique
- 3% Man in the middle

Source: PwC's 2018 Global Economic Crime Survey – New Zealand respondents

[8] Attacks using open source intelligence to gather information about an individual to craft unique and highly convincing emails.

Anti-Money Laundering (AML)



Beyond ticking boxes

As the regime matures, greater numbers of Reporting Entities are requiring assistance with remediating inadequate AML/CFT Risk Assessments and Programmes. Reporting Entities put themselves at considerable risk by adopting a 'tick the box' approach and our survey showed that 24% of Reporting Entities surveyed did not consider it is necessary to perform an AML/CFT Risk Assessment. This may indicate some Reporting Entities treat their risk assessments as static documents, contrary to the requirements of the Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act 2009 (the Act).

40% of reporting entities indicated they had experienced regulatory enforcement or inspection related to AML/CFT in the last two years, so getting it wrong is a real regulatory risk. Remediation under pressure of regulator action is much more costly and time-consuming for management than getting it right proactively.

For those organisations who are starting their AML/CFT journey, this is a time-consuming, costly, and stressful undertaking, especially if left to the last minute.

Methods of money laundering continue to evolve, and with the rise of products and services which facilitate anonymous payment and receipt of goods, such as cryptocurrencies, reporting entities must continue to assess where their risks are and how they will respond and ensure their customer due diligence procedures are sufficient.

Risk assessment

Has your organisation performed an AML/CFT (Anti-Money Laundering/Combating Financing of Terrorism) risk assessment across its business and geographies in the last 24 months?

Source: PwC's 2018 Global Economic Crime Survey

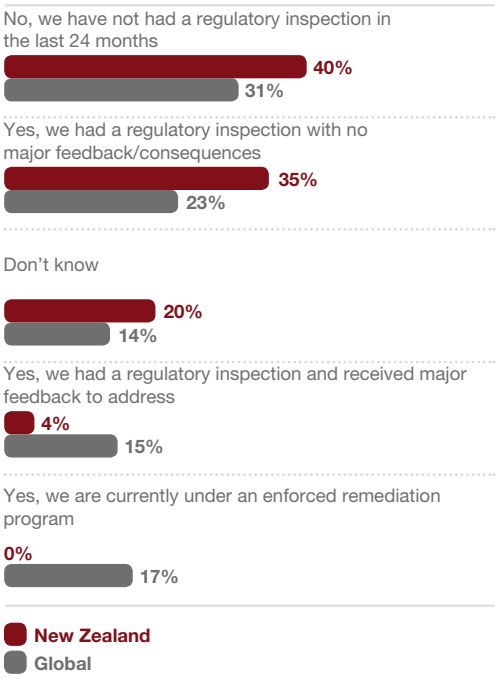
Across the board, regulations and reporting requirements, touching on both legal and ethical behaviour, continue to expand. Scrutiny and enforcement are also on the rise globally, and cross-border regulatory cooperation is becoming increasingly routine.

Phase one of New Zealand's Anti-Money Laundering regime came into force on 30 June 2013, impacting financial institutions and casinos. As Reporting Entities, financial institutions must comply with the requirements of the Act. The regime continues to have a significant impact on a wide range of reporting entities, such as banks, finance companies, non-bank deposit takers, as well as many other businesses and their customers. But the regime is now changing.

From mid 2018 lawyers, accountants, real estate agents, high-value dealers and the New Zealand Racing Board are being progressively brought into the regime. Being prepared for becoming a reporting entity is critical to ensuring compliance from day one. The introduction of these new classes of Reporting Entities is at a time when the existing regime is still not fully mature.

Regulatory enforcement

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



Source: PwC's 2018 Global Economic Crime Survey

With reporting entities now being taken to task for non-compliance with the NZ AML/CFT Legislation, compliance is no longer a 'tick the box' exercise, but a task to take seriously.

Conclusion

Be prepared – and emerge stronger

Transparency is at the heart of the economic crime problem in New Zealand.

While economic crime will always be part of the business landscape, there are many opportunities to lower that exposure, detect and investigate offenders and use those experiences as a virtuous learning circle. An investment in understanding your organisation's blind spots and identifying risks, followed by targeted changes in your approach to your use of technology and organisational culture offers the best prospects. Our survey results clearly show that there is more to be done in all of these areas.

The threat of economic crime continues to intensify and the rules and expectations of all your stakeholders – including regulators, shareholders, the public, especially through social media, and employees – have increased and will continue to do so. Transparency and adherence to the rule of law are more critical than they have ever been and how you respond when a fraud or compliance issue arises is as important as the event itself.

Taking deliberate actions to plan, prevent, detect and remediate are key. Whether this be to meet your statutory requirements such as a whistleblower service or meeting your AML/CFT obligations, developing a comprehensive organisation-wide fraud control framework or cybercrime strategy, the costs and management distraction of not being active will almost certainly outweigh the up-front costs.

Actively managing your economic crime risks gives you a competitive advantage in an increasingly demanding market looking for organisations with a strong ethical frameworks and transparency.

What next?

If you want to know more about any of the issues discussed above, be it fraud or bribery risk, cybercrime, forensic technology, AML or integrity due diligence, then please contact one of our subject matter experts.

About the survey

PwC's 2018 Global Economic Crime and Fraud Survey was completed by 7,228 respondents from 123 PwC territories including New Zealand. Of the total number of respondents, 52% were senior executives of their respective organisations, 42% represented publicly-listed companies and 55% represented organisations with more than 1,000 employees.

Stephen Drain
Partner
Forensic Services
+64 9 355 8332
stephen.c.drain@nz.pwc.com

Campbell McKenzie
Director
Forensic Technology Solutions
+64 9 355 8040
campbell.b.mckenzie@nz.pwc.com

pwc.co.nz/crimesurvey2018