

Adjusting the lens on economic crime

Preparation brings opportunity back into focus



40%

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

55%

of NZ organisations don't have an operational cybercrime incident response plan

42%

of NZ organisations' fraud events are detected by tip-offs



Contents

5 **Foreword**

6 **Leading observations**

8 **New Zealand findings**

- What does this year's survey tell us?
- What type of economic crime was reported?
- Which industries are at risk?
- Financial damage
- Who is the fraudster?

28 **Ethics and compliance**

- Aligning values and strategy with risks and responsibilities
- People & culture: your first line of defence
- Aligning roles & responsibilities: who's in charge here?
- Fraud – opportunities for the fraudster – and you
- Implementing in high-risk areas: the devil is in the details

16 **Cybercrime**

- When connectedness becomes ubiquitous, so do threats
- Expanding the definition
- Cybercrime keeps climbing – damage is not just financial
- The importance of a multi-layer defence
- The responsibility of the entire organisation

36 **Anti-money laundering**

- Are you prepared for the regulatory environment?
- The reputational and regulatory risk in New Zealand
- Money laundering destroys value
- AML: the pace of regulatory change
- What does this all mean for New Zealand reporting entities?



Welcome to our New Zealand supplement to PwC's 2016 Global Economic Crime Survey

As well as updating the overall picture on economic crime in New Zealand, we focus this year on cybercrime, ethics and compliance, and anti-money laundering programmes, with the opportunity to improve performance simply by being ready to deal with the threats we face.

The overall picture for New Zealand continues from our previous survey:

- Well over one-third of respondents experienced economic crime;
- Notwithstanding an emphasis on cybercrime, the biggest issue by a substantial margin remains asset misappropriation;
- Detection rates by corporate controls have fallen and we remain heavily reliant on tip-offs;
- In a fast-changing and digitally dependent market, many organisations are not well placed to avoid cybercrime attacks, or if subject to attack, respond to them. Further, while the tone from the top on ethics is positive, the message does not always flow right through the organisation;
- We also deal with anti-money laundering this year, where compliance with our relatively new legislation has been a challenge for many financial institutions who are now covered. We remain behind the rest of the world in implementing AML legislation, and you should expect its influence to extend into the business world significantly further in years to come.

These issues challenge you to adjust your lens on economic crime and refocus your path towards opportunity around strategic preparation. Strategic in that it is related and interwoven from the daily activities of the business unit up into the ethical fabric of the company. Ensuring your company is prepared for success in today's world is no longer an exercise in producing plans which, once prepared, never see the light of day. In a fast-moving digital world, being prepared is a living, breathing daily exercise which needs to be constantly updated so you are ready when threats turn into reality.

Understanding your vision and strategically maintaining a plan for growth as well as defence will be the difference between taking your opportunities or allowing those who want to victimise you to capitalise on theirs.

Eric Lucas
Forensic Services Partner
PwC New Zealand



Leading observations for New Zealand

1 Economic crime is an obstinate threat

- 40 per cent of organisations experienced economic crime (up from 33% in 2014) but the key types are unchanged – asset misappropriation is the most common
- Corporate detection methods are not keeping pace

What opportunities are available for proactively countering economic crime?



Reported economic crime similar to 2014 rate

4 Opportunity is the main driver for internal economic crime

- Almost half (44%) of the incidents of serious economic crimes were perpetrated by internal parties
- Organisations need to ensure that there is not a disconnect between the tone at the top and the reality on the ground
- 72 per cent of CEOs are planning to make changes in their values, ethics and codes of conduct

Do all members of your organisation work towards the same compliance outputs?



People and culture are your first line of defence

2 Cyber threats climb, but business preparation is not keeping pace

- Cybercrime tied with procurement fraud for the second-highest type of economic crime experienced in New Zealand at 29 per cent
- Most companies are still not adequately prepared for or even understand the risks: Only 45 per cent of organisations have a cyber-incident response plan
- Only around half of board members request information about their own organisation's state of cyber-readiness

How will your cyber-response plan stand up to reality?



Cyber preparedness can be viewed as an organisational stress test

5 Anti-money laundering (AML) compliance – the pace of regulatory change and the lack of skilled personnel are the greatest challenges

- The AML net is set to expand in New Zealand
- New Zealand reporting entities still have many challenges to fully comply
- Globally, one in five of financial-services respondents needed to address significant issues after regulatory inspection
- Cost of compliance continues to rise

How would your organisation fare in the face of regulatory scrutiny?



Have you considered the growing impact of the AML regime?

3 Financial crime compliance risk is on the rise

- Asset misappropriation remains the biggest threat
- Corporate controls aren't identifying the problem
- 42 per cent of fraud detection is through a tip-off, including a formal whistleblower service
- 67 per cent of organisations say they have a formal business ethics and compliance programme
- Tone from the top on ethics doesn't always flow through the organisation

Can your compliance programme foresee and address an evolving risk landscape?



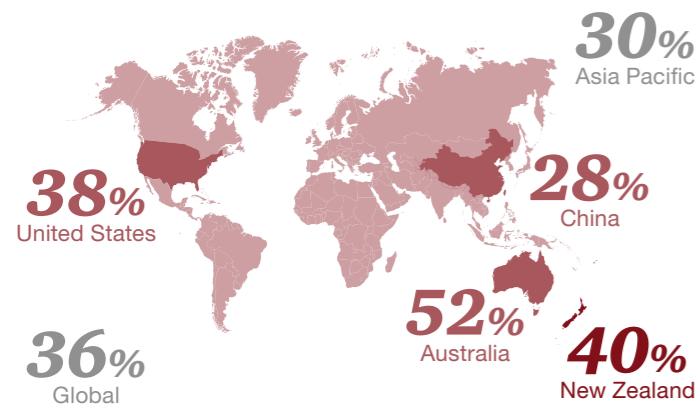
Bribery and corruption is low in New Zealand but not so with our major trading partners

Economic Crime in New Zealand

What does this year's survey tell us?

Of the 85 New Zealand respondents to our survey, 40 per cent have experienced economic crime in the past 24 months. This ranks New Zealand 19th out of 115 countries that took part in the survey, and places us slightly above the global average of 36 per cent and below our neighbours Australia (52%). This year's survey results show that the rate of reported economic crime has remained largely unchanged this century.

Percentage of organisations experiencing fraud

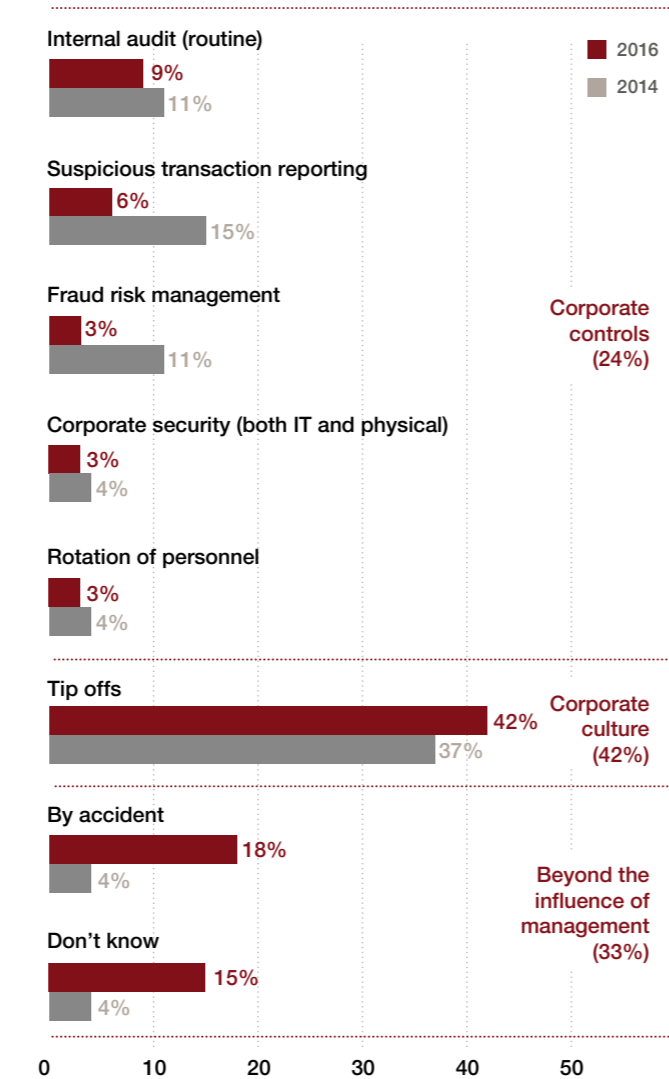


The persistence of this trend over the 15 years since our first Global Economic Crime Survey (2001) bears testimony to the obstinate threat that economic crime represents.

New Zealand ranks 19th out of 115 countries that took part in the survey

Once again, our survey finds that the most common method of identifying economic crime is via some form of tip-off (42%), including a formal whistleblower service. This has important ramifications for organisation's fraud detection systems. This survey has seen a decrease in the detection of criminal activity by methods within management's control (corporate controls detection is down from 56% to 24%). What's more, one in five organisations (18%) have not carried out a fraud risk assessment in the last 24 months.

Detection methods in New Zealand



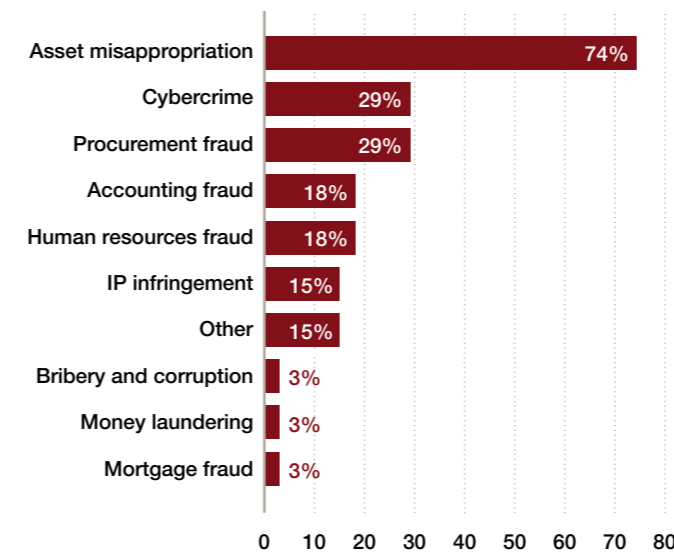
In PwC's 2016 New Zealand CEO Survey¹ two-thirds (66%) of chief executives agreed that there are more threats to the growth of their company than three years ago. This points to a potentially worrying trend – including that 18 per cent of all economic crimes detected in New Zealand were 'by accident'. Today more than ever before, a passive approach to economic crime is a recipe for disaster.

What type of economic crime was reported?

Asset misappropriation continues to be the most common economic crime reported in New Zealand. This year's level of 74 per cent is consistent with our last two surveys and shows that despite an increase in cybercrime and procurement fraud in recent years, it remains a top threat for New Zealand organisations.

As we discuss below, that while organisations need to ensure that they are ready for the growing and increasingly complex threats from cybercrime – now in joint second place as the most reported economic crime – they cannot afford to take their eye off the traditional frauds and thefts.

Types of economic crime experienced in New Zealand



New Zealand's results are broadly consistent with the global findings with one exception: only 3 per cent of respondents reporting instances of bribery and corruption, compared to a global incidence of 24 per cent.

That New Zealand's incidence of reporting bribery and corruption is low by global standards reflects a generally transparent and honest business culture. This is also demonstrated in our regular high ranking in transparency indices.²

However, New Zealand businesses dealing with our trading partners are at a higher risk.

Reports of bribery and corruption in New Zealand's three largest trading counterparts – China, Australia, and the United States – are more significant. Many jurisdictions including the US and UK have specific anti-bribery and corruption requirements for businesses which operate in or with them. Without local experience to fall back on, trading in an environment where bribery and corruption are frequent risks requires careful planning, not just to meet regulatory requirements, but to know what to do when faced with an event.

CEOs are starting to be engaged: Our recent CEO Survey showed 19 per cent of CEOs in New Zealand were concerned with the threat of bribery and corruption as a threat to business growth.

Bribery reported in New Zealand's top three trading nations



Note: New Zealand reported 3 per cent

Are we still prepared for traditional fraud and theft in the workplace?

1 2016 Annual New Zealand CEO Survey

2 For example, the Transparency International Corruption Perception Index

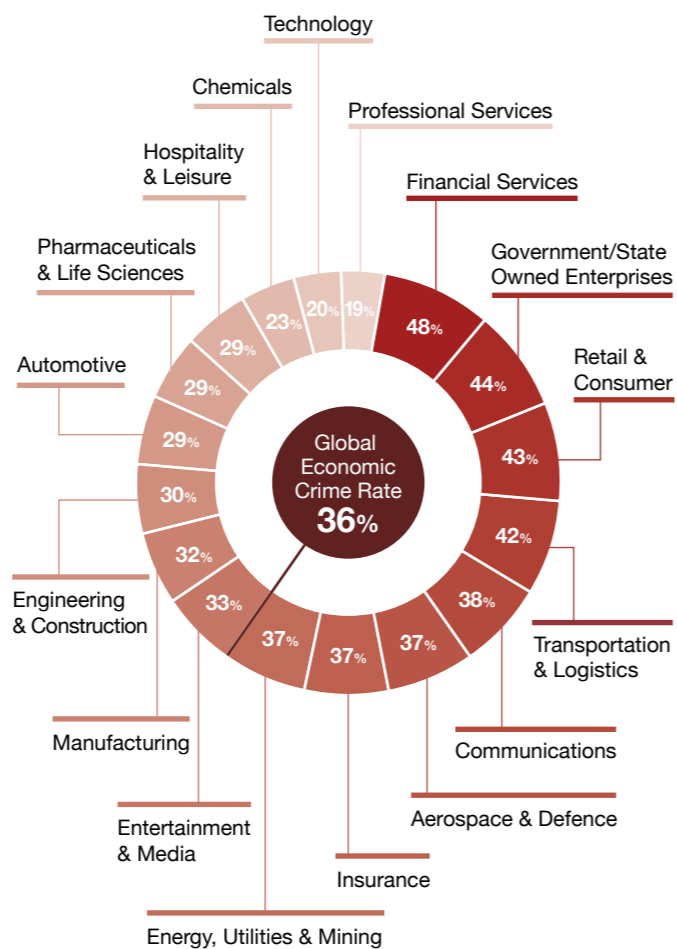


Which industries globally are at risk?

Globally, financial services has traditionally proven to be the industry most susceptible to economic crime. However, with the market evolving towards integrated business solutions, many non-financial services organisations are now providing in-house financial solutions. Many of these businesses – automotive, retail and consumer and communications sectors – have become hybrids with either joint arrangements with financial services companies or financial licences of their own. This means that fraudsters who follow the cash now have many more avenues to fulfil their objectives.



Percentage of organisations experiencing economic crime in the past two years



Source: All global respondents

While the financial services industry, by virtue of its highly regulated environment, has over the decades built up sophisticated control mechanisms, detection methodologies and risk management tools, the hybrids have generally yet to come into their own in managing the risks and the fast-evolving compliance landscape they now find themselves in. This is particularly so for reporting entities captured by New Zealand's anti-money laundering legislation. We explore this area further in our anti-money laundering section (see page 36).

Financial damage

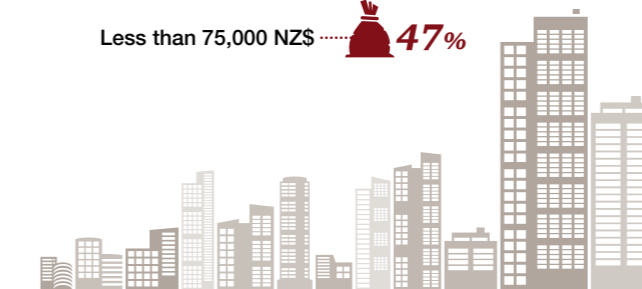
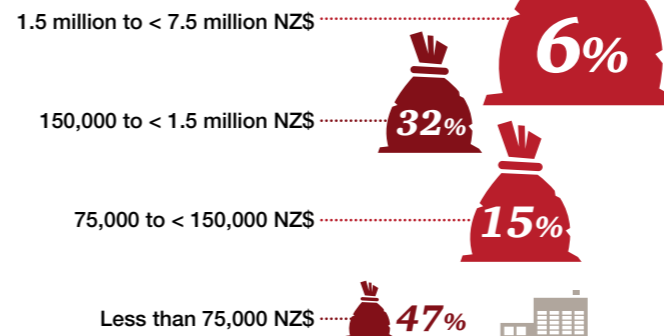
While around half of reported instances were losses of less than NZ\$75,000, around 40 per cent were losses in excess of NZ\$150,000. In a country of small businesses, such losses can have a significant impact on the affected entity.

Globally, 25 respondents who reported as having experienced a loss, said that the loss was in excess of US\$100 million.

The true cost of economic crime to the New Zealand economy is difficult to estimate, especially considering that actual financial loss is often only a small component of the fallout from a serious incident. Business disruption costs, remedial measures, investigative and preventative interventions, regulatory fines and legal fees all have an impact on the bottom line, and these costs can be large and not easily quantifiable.

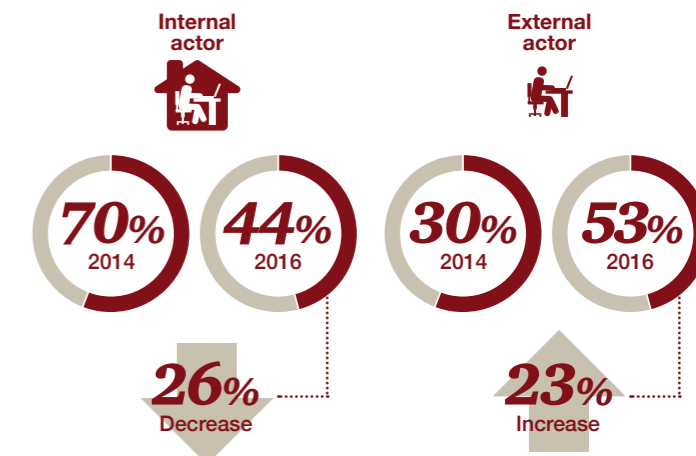
Financial impact of economic crime in New Zealand

In financial terms, approximately how much do you think your organisation may have lost through incidents of economic crime over the last 24 months?



Who is the fraudster?

Employees acting against their own organisations make up 44 per cent of New Zealand's fraudsters.



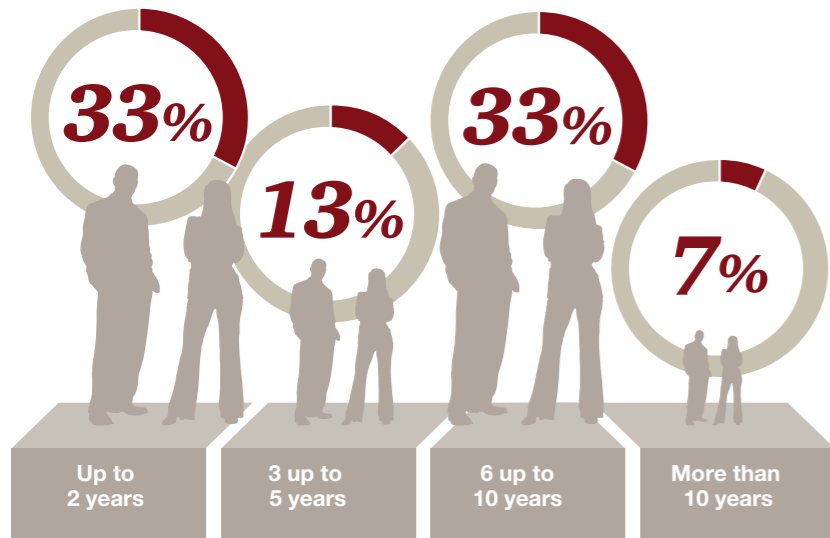
Four in 10 internal perpetrators originate from junior management, but middle and senior management also contributed a great deal to the perpetration of internal fraud. This points to a potential weakness in internal controls whereby these measures can serve as "check-box" exercises rather than effective processes embedded into an organisation's culture. It is interesting to note that 18 per cent of respondents did not carry out a fraud risk assessment during the 24-month period surveyed. We explore this area further in our ethics and compliance section.

Now more than ever organisations have the opportunity to rethink their control structures and go back to fundamentals. Creating a culture of controls and risk awareness rather than ritualised activity, supplemented by zero tolerance for dishonest practices, can help insulate organisations from avoidable losses due to internal fraud.

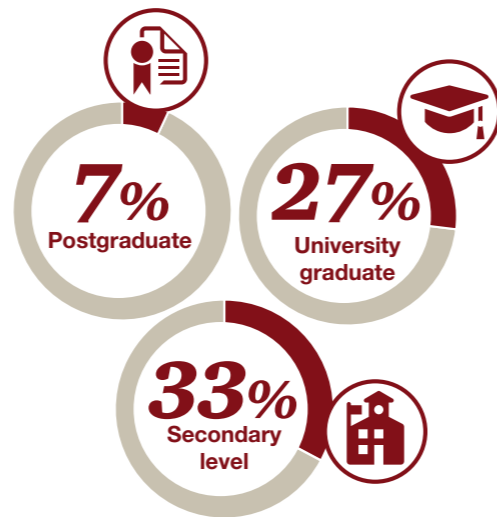


Typical profile of the fraudster in New Zealand

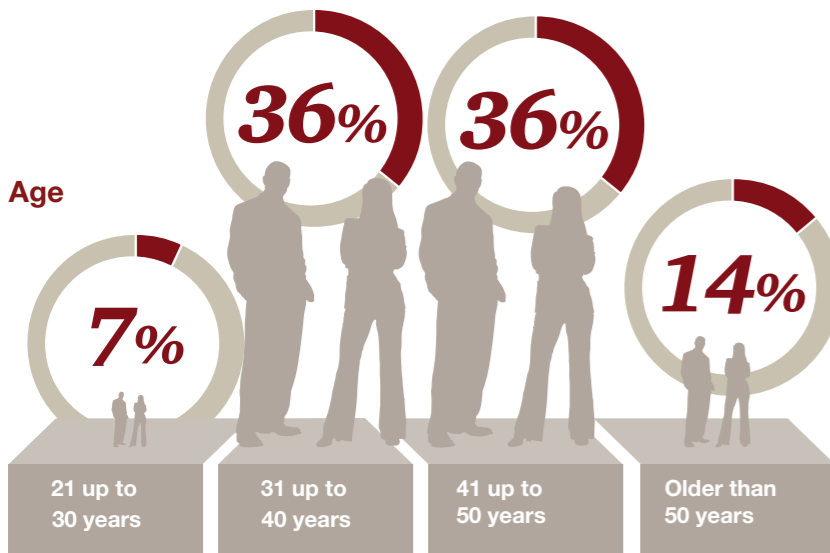
Length of service



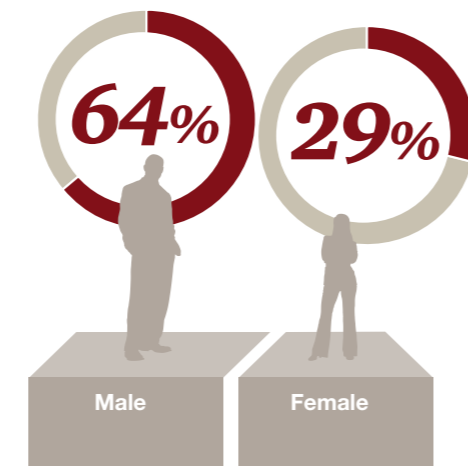
Education level



Age



Gender



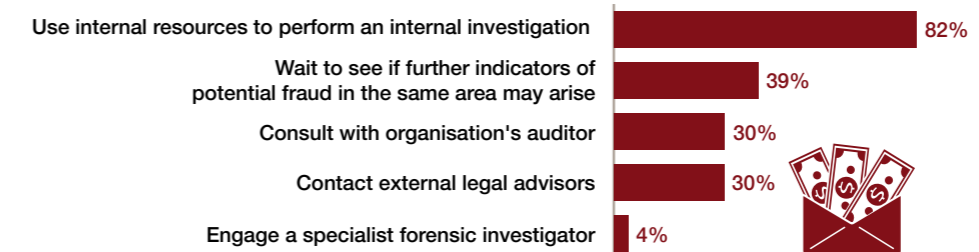
Note: Numbers may not add to 100 per cent as some respondents stated "don't know".



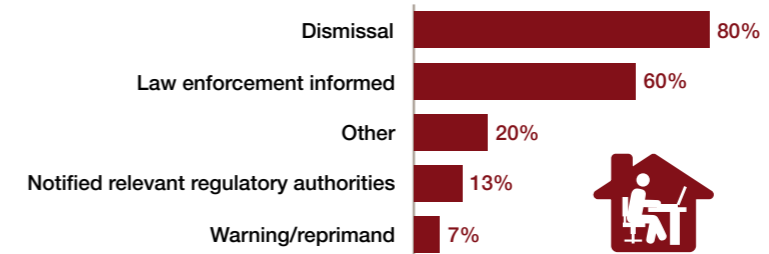


Actions taken against fraudsters in New Zealand

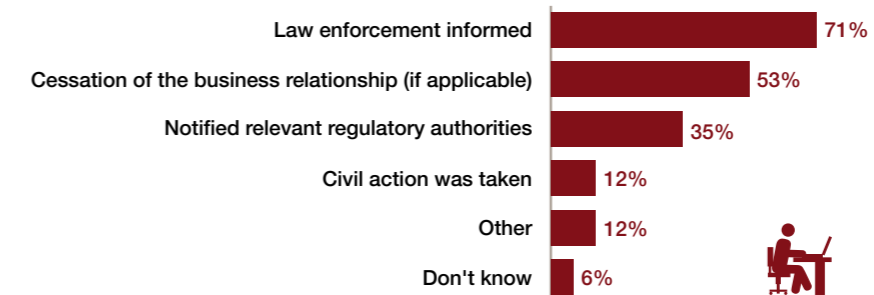
When an incident of potential fraud is identified, which action(s) are likely to be taken?



What actions are taken against the main internal perpetrator?



What actions are taken against the main external perpetrator?



Turning opportunity for crime into opportunity for growth

We focus now on strategic opportunity. What does the data really mean for your business, going forward? Our survey numbers can help uncover potentially troublesome red flags and trends and serve as important indicators of areas of opportunity for forward-thinking organisations. These are discussed in the three upcoming sections: cybercrime, anti-money laundering, and ethics and compliance programmes.



Cybercrime

When connectedness becomes ubiquitous, so do threats

Digital technology continues to transform and disrupt the world of business, exposing organisations to both opportunities and threats. So it's hardly surprising that cybercrime continues to escalate.

The reality in 2016 is that like every other aspect of commerce, economic crime has, to some extent, gone digital.

Here's the digital paradox: organisations today are able to cover more ground, more quickly, than ever before – thanks to new digital connections, tools and platforms which can connect them in real time with customers, suppliers and partners. Yet at the same time, cybercrime has become a powerful countervailing force that's limiting that potential.

This elevated level of awareness about the growing encroachment of cybercrime is confirmed in our 2016 Annual New Zealand CEO Survey, where in New Zealand, nearly eight in 10 (77%) chief executives expressed concern – from moderate to extreme – about this threat.

This year's Global Economic Crime Survey points to the disquieting fact that too many organisations are leaving first response to their IT teams without adequate intervention or support from senior management and other key players. What's more, the composition of these response teams is often fundamentally flawed, which ultimately affects the handling when a breach occurs.

We've come a long way from the days of teenaged hackers stealing bank cards. There's been a significant and laudable increase in awareness and sophistication in detecting the identity (or provenance) of an attacker. Still, the fact remains that the conflict between criminals and companies is as feverish as ever. For companies, it's a battle that can never be completely won.

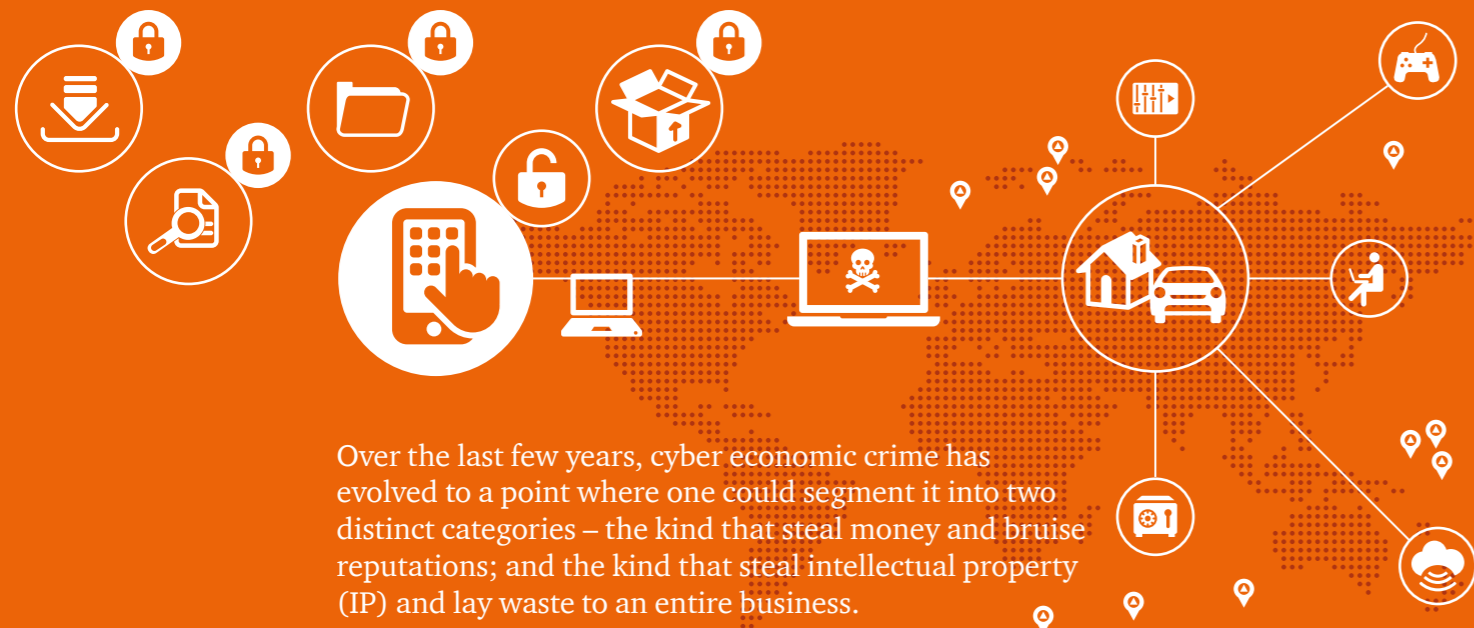
Expanding the definition

Cybercrime, also known as computer crime, is an economic offence committed using the computer and internet. Typical instances of cybercrime are the distribution of viruses, ransomware, phishing, whaling and theft of personal or confidential information. This excludes routine fraud whereby a computer has been used as a by-product in order to create the fraud and only includes such economic crimes where computer, internet or use of electronic media and devices is the main element and not an incidental one.

Over the last few years, cyber economic crime has evolved to a point where one could segment it into two distinct categories – the kind that steal money and bruise reputations; and the kind that steal intellectual property (IP) and lay waste to an entire business.

- Cyber fraud. Monetisable cybercrime, such as identity and payment card theft, are the events that tend to grab the headlines, with millions of dollars of losses and as many victims. Despite their high profile, they rarely pose an existential threat to companies.
- Transfer-of-wealth/IP attacks. The more critical economic crime facing organisations is that of cyber espionage: the theft of critical IP, trade secrets, product information, negotiating strategies and the like. Cyber professionals call such breaches 'extinction-level events,' and for good reason. The damage could extend to the billions of dollars, and include destruction of a line of business, a company or even a larger economic ecosystem. Not only are these kinds of attacks difficult to detect, they may not even be on a company's threat radar.

While the long-term damage, both to the entity and the economy, is potentially far higher for transfer-of-wealth attacks, the regulatory pain and media scrutiny arising from the theft of credit cards or personally identifiable information can be vast.



Over the last few years, cyber economic crime has evolved to a point where one could segment it into two distinct categories – the kind that steal money and bruise reputations; and the kind that steal intellectual property (IP) and lay waste to an entire business.

1000101011011000010111010101010110001010101000101101001010010100011101
010010110101010010011000010111100001101010101011101011010000111010101101
0101010111100010101000000111010101010101001111010000101111000011110000
010101010101010100101010100111110000111111000110010010001001001001101



Cybercrime continues to escalate in a hyperconnected business ecosystem – jumping to joint second most reported economic crime in New Zealand

Cybercrime jumps to the joint second most reported economic crime...

29% of New Zealand organisations affected by economic crime have experienced cybercrime

...and another **12%** said they didn't know if they had or not

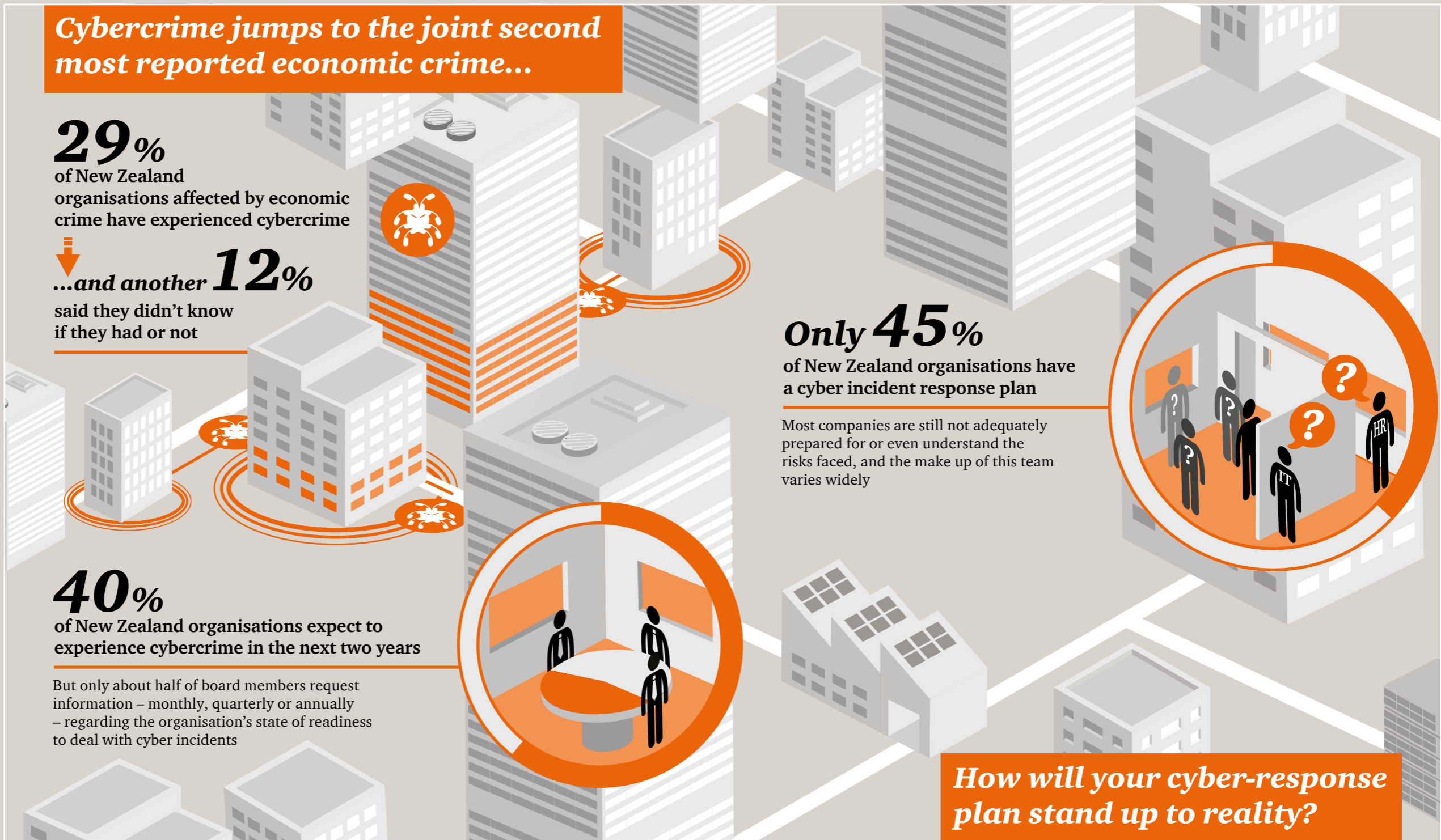
40% of New Zealand organisations expect to experience cybercrime in the next two years

But only about half of board members request information – monthly, quarterly or annually – regarding the organisation's state of readiness to deal with cyber incidents

Only 45% of New Zealand organisations have a cyber incident response plan

Most companies are still not adequately prepared for or even understand the risks faced, and the make up of this team varies widely

How will your cyber-response plan stand up to reality?





So where's the opportunity here? It is in staying one step ahead of the threat. That requires a clear-eyed understanding of the shape of the threat as it relates to your particular industry, and being prepared to respond, top to bottom, as a single organisation.

As well as elongating the interval between successful attacks, it is also critical to shrink the interval between effective detection and response – and thus interrupt damaging business impacts as quickly as possible. This can be a powerful argument to tie back to board conversations.

Cybercrime keeps climbing – damage is not just financial

The incidence of reported cybercrime among our respondents is sharply higher this year, jumping from fifth to joint second place among the most-reported types of economic crime in our 2016 survey, compared to 2014 results. Over a quarter (29%) of respondents told us they'd been affected by cybercrime, and another 12 per cent said they didn't know whether they had or not.

Losses can be heavy with several local respondents reporting losses of over NZ\$150,000. Globally 43 organisations reported losses of over NZ\$7,500,000.

Among the global survey respondents, reputational damage was considered the most damaging impact of a cyber-breach.

In New Zealand, participants concerned about the impact of regulatory risks may in part be associated with the proposed changes to the Privacy Act relating to the mandatory notification of data breaches. Also worth noting are New Zealand's concerns around the impact resulting from the theft of personal information and the theft of intellectual property. These concerns are consistent with what our clients have told us while assisting them over the same 24-month survey period.

What industries are at risk for cybercrime?

Today, all industries are at risk – including some which may have considered themselves unlikely targets in the past. According to PwC's *Global State of Information Security Survey 2016*, the sector registering the most significant increase in cybercrime activity in 2015 was retail, while financial services – still one of the most attacked sectors – had levelled out, with very little growth in terms of number of attacks over the last three years.



Composition of first responder teams across the globe



Source: All global respondents

New Zealand view on data breaches – How ready is your incident response plan?

A common type of cybercrime which is fast becoming ubiquitous is a data breach or data theft and unfortunately, New Zealand organisations are not immune.

So what is being done in New Zealand to prevent, detect and respond to the threat of a data breach?

The position of data owners has recently been strengthened as the Supreme Court of New Zealand determined that the theft of electronic data is, in fact, a criminal offence. The Court found that data is property, and the theft of it is illegal.

Unfortunately for victims, the process of responding to a data breach is not straightforward, often requiring the urgent preservation and examination of electronic evidence, and in many cases requiring specialist forensic expertise. The impact can be profound, mitigated in part by an organisation's ability to manage its reputational damage once word of a breach starts spreading. As a data breach often consists of personal information, New Zealand privacy laws are gearing up for a change to be more in line with US laws where reporting a breach may become mandatory.

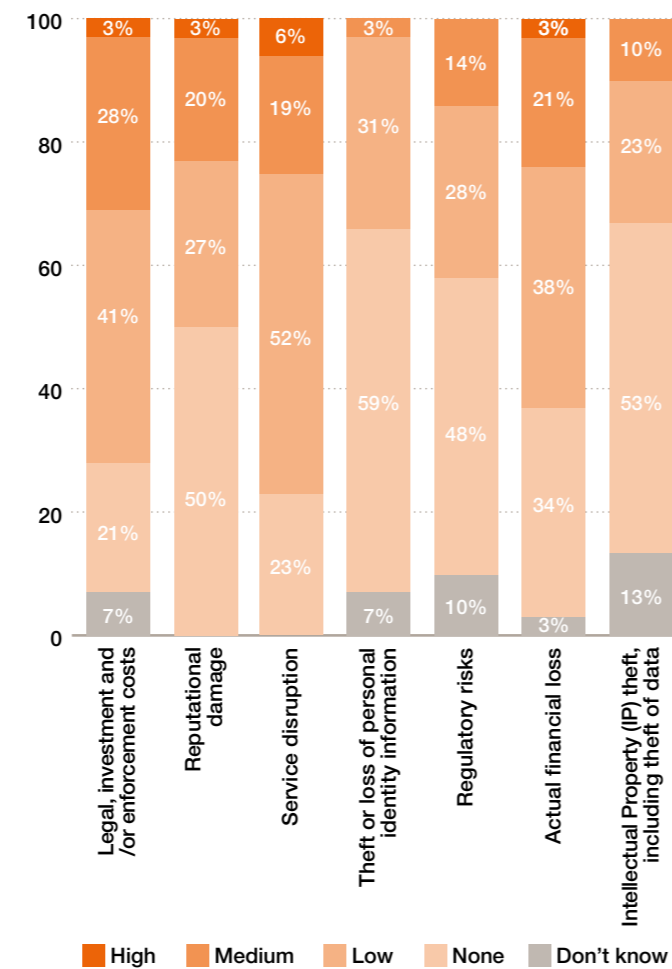
In the 2016 Annual New Zealand CEO Survey, 77 per cent of CEOs indicated cyber threats as a top threat to business growth in the coming year. So it's unsurprising to see that a significant number of boards are now regularly asking for information on the state of readiness to deal with cybercrime incidents. It is encouraging to see that many of our respondents are implementing an incident response or first responder plan – but how will the remainder respond and perform in their time of crisis?

Of the organisations with an internal incident response capability, only 9 per cent have a digital forensic investigator on the team. Finally, the New Zealand Government's recently released Cyber Security Strategy 2015 recommends the establishment of a national Computer Emergency Response Team. Digital disruption is a threat that every business faces.

When is the last time you thought about your incident response plan?




Level of impact of cybercrime in New Zealand (for organisations reporting a cyber-incident)




The insidious nature of cybercrime is such that a percentage of the 51 per cent who say they are not victims have likely been compromised without knowing it. A concerning trend we have observed is that hackers manage to remain on organisations' networks for extended periods of time without being detected. Attackers also are known to stage diversionary attacks to conceal more damaging activity.


Threat vectors: the five categories



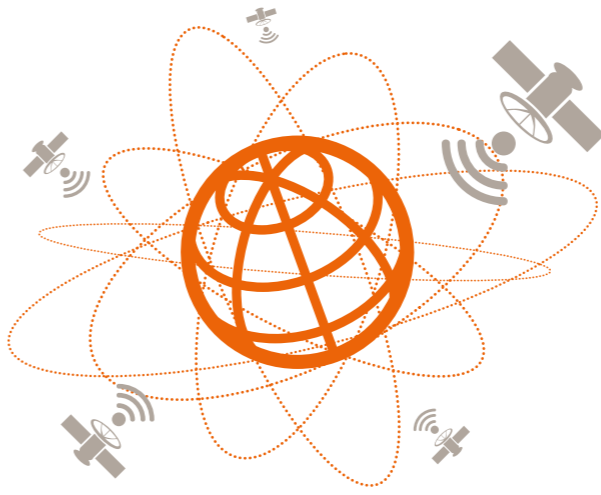
Nation-states
threats include espionage and cyber warfare; victims include government agencies, infrastructure, energy and IP-rich organisations




Insiders
not only your employees but also trusted third parties with access to sensitive data who are not directly under your control




Terrorists
still a relatively nascent threat, threats include disruption and cyber warfare; victims include government agencies, infrastructure and energy





Organised crime syndicates
threats include theft of financial or personally identifiable information (sometimes with the collusion of insiders); victims include financial institutions, retailers, medical and hospitality companies



Hacktivists
threats include politically focused service disruptions or reputational damage; victims include high-profile organisations, governments or individuals

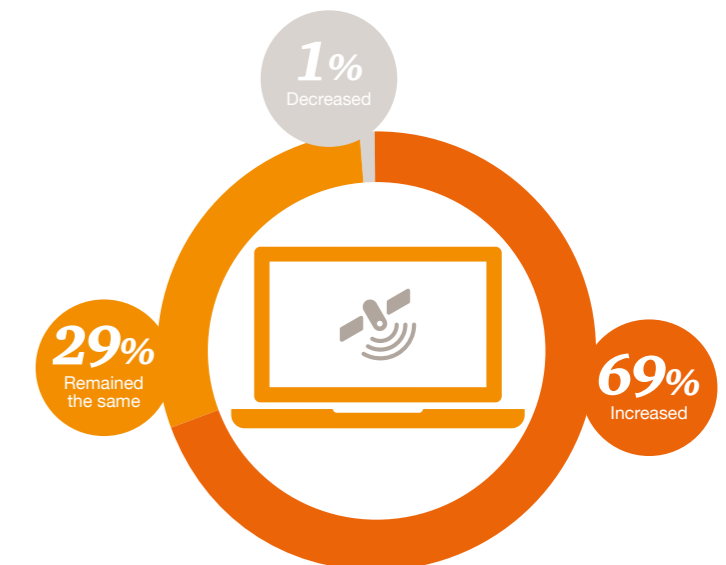
Why do companies (and nation-states) steal intellectual property?

- Many developed nations are seeing a pattern in large-scale IP-focused breaches. They are not random individual company attacks, but rather parts of a larger-scale, strategically organised campaign.
- While nation-states may be behind some of these large-scale attacks, this is not a terrorism issue (attempting to cripple vital infrastructure), it is an economic crime issue.
- There is an economic rationale in stealing another company's intellectual property. It is less expensive in time and resources than conducting one's own research and development. The advice is: if you see someone else in your sector getting attacked, it is wise to assume you may be next.

Ready or not

Over half of our survey respondents in New Zealand (69%, up 21% since 2014) see an increased risk of cyber threats, perhaps due to intensifying media coverage. But our survey suggests that companies are nonetheless inadequately prepared to face current cyber threats.

How has your perception of the risks of cybercrime to your organisation changed over the last 24 months?

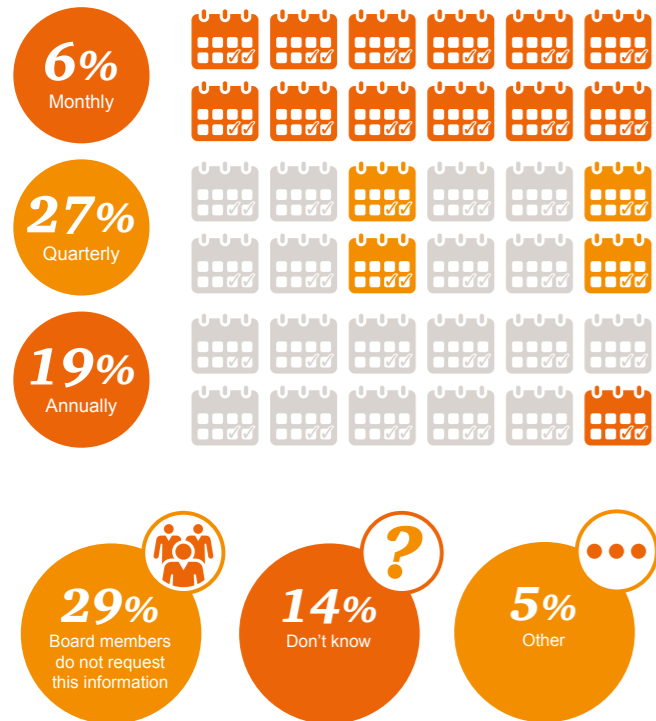


Source: New Zealand respondents



Responsibility for redressing cyber vulnerabilities starts at the top. Yet our survey suggests that many boards are not sufficiently proactive regarding cyber threats. Around half of board members actually request information about their organisation's state of cyber-readiness on a quarterly, monthly or annual basis.

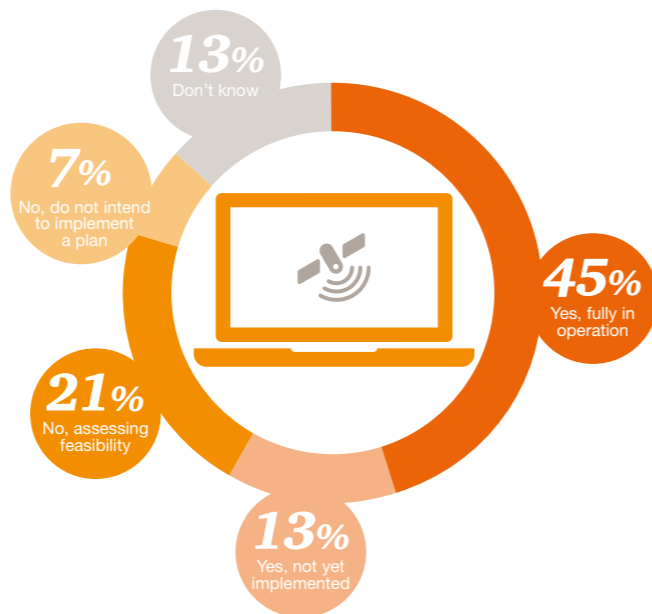
How often do board members request information regarding the organisations state of readiness to deal with cyber incidents?



Source: New Zealand respondents

Only 45 per cent of respondents have a fully operational incident response plan. Three in 10 (28%) New Zealand organisations have no plan at all, and of these, a quarter don't think they need one.

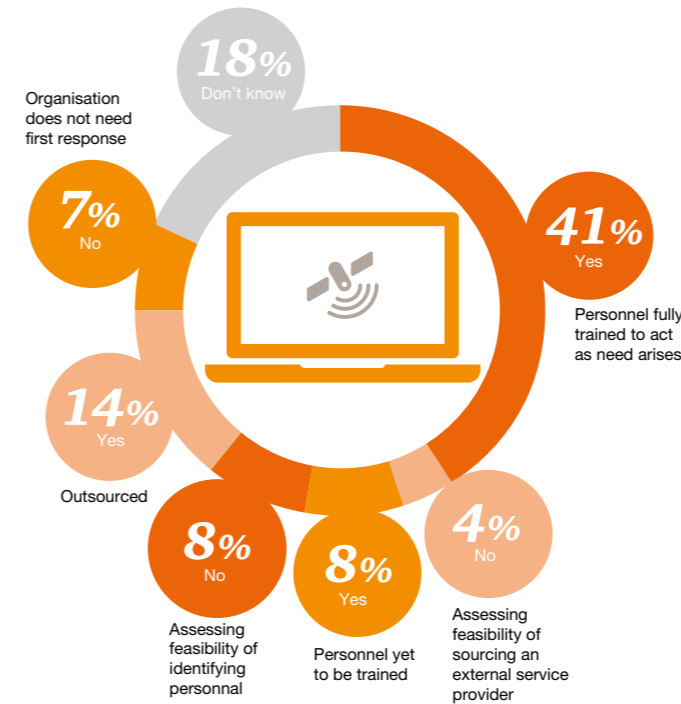
Do organisations have an incident response plan to deal with cyber attacks?



Source: New Zealand respondents

Should a cyber-crisis arrive, only four in 10 companies have personnel fully trained to act as first responders – of which the majority (74%) are IT staff.

Have organisations identified cyber breach first responder teams?



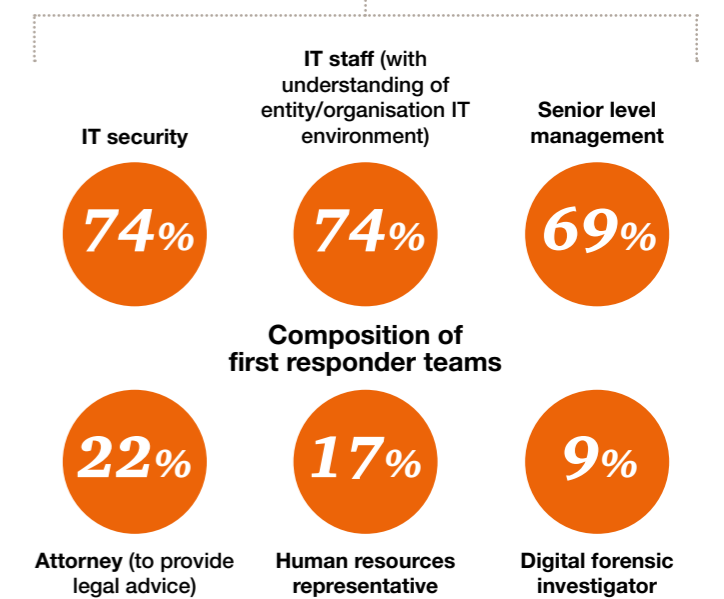
Source: New Zealand respondents

While IT has a critical role to play in detecting and attempting to deflect an attack, it is noteworthy that first responder teams in New Zealand generally lack involvement from legal (22%) and HR (17%) members. Only one in 10 (9%) incident response teams included digital forensic investigators.

These results suggest that many organisations, in their understandable haste to contain the breach and get their systems up and working again, are at risk of overlooking potentially crucial evidence – which could later hamper their ability to prosecute and, more importantly, to understand how the breach occurred.

Excessive haste in responding to an attack can hamper the company's ability to fully understand the holistic impact of the breach – and communicate appropriately to both internal and external stakeholders, including the media. This could lead to reputational harm.

Composition of first responder teams in New Zealand



Source: New Zealand respondents



Data breach incident response action plan

What happens when you learn of a data breach? It's critical to shrink the interval between effective detection and response – and interrupt the damage to your organisation as quickly as possible. After calling up your crisis and cyber first responders, here are some steps you can take:

1. Establish the essential facts about the breach, and find out if it is still ongoing. Sophisticated forensic and data analytical tools are critical during this phase.
2. Consider that the detected attack may in fact mask other infiltrations into your organisation, and that in certain situations it may take weeks, not hours, to determine the full extent of the problem and begin to stem the damage.
3. Decide whether to involve law enforcement. There are many factors to consider, and they will vary according to the type and scale of the attack.
4. Consider secondary risks. For example, a simple email breach may reveal confidential information to adversaries.
5. Finally, when a breach occurs, remember that: a cyber investigation is still fundamentally an investigation, and the principles of a criminal investigation still apply. In focusing on stopping an ongoing attack and getting back on line, it's crucial not to inadvertently destroy evidence that could help with that investigation and with preventing the next attack.

The importance of a multi-layered defence

While we have seen major strides in sophistication and cyber-preparedness since our last survey, most companies are still not adequately prepared either to understand the risks they face, nor to anticipate and manage incidents effectively.

Too many organisations are suffering cyber losses because they didn't get the basics right. From insufficient board involvement (or readiness-awareness), to poor system configurations and inadequate controls on third parties with access to the network, companies are suffering from unforced errors, often leaving the cyber door ajar for intruders.

Responsibility for redressing cyber vulnerabilities starts at the top. Yet our survey suggests that many boards are not sufficiently proactive regarding cyber threats, and generally do not understand their organisation's digital footprint well enough to properly assess the risks.

It is vital that boards incorporate cybercrime into their routine risk assessments. Especially in the light of the kinds of virulent IP attacks that could take a company down, boards and senior management must continuously ask themselves if they are adequately prepared to deal with these kinds of large-scale attacks. Crucially, they must also communicate clearly to the IT department at what point they want to be alerted of a breach.

Organisations seeking further assistance may refer to the Institute of Directors in New Zealand, who recently published the Cyber-Risk Practice Guide. This guide provides boards with principles to help them understand and monitor cyber-risk, develop strategies for seeking assurance, and oversee management.

Ultimately of course, cyber threats and mitigations are the responsibility of the entire enterprise; all have a crucial part to play. There's room for improvement at all levels of your organisation and, unlike the frequency of external cyber-attacks, this is something you can control. An investment in preparedness – the ability to identify the potential for cyber-attack, prevent it wherever possible, and detect it when it's not – can pay dividends in damage minimisation.

All organisations today require a foundational level of cyber preparedness (or 'digital hygiene'), beyond which the level of investment in preparedness should be determined by their individual risk profile.

Regardless of the sector, the crucial point is that preparedness for cybercrime must be embedded within the wider scope of crisis planning, not separate from it.

Cyber threats must be understood and planned for in the same way as any other potential business threat or disruption (such as acts of terrorism or a natural disaster) with a response plan, roles and responsibilities, monitoring and scenario planning.

A cyber corporate crisis is one of the most complex and challenging issues an organisation can face. Cyber breaches require sophisticated communications and investigative strategies – including significant forensic and analytical capabilities – executed with precision, agility and a cool head.

Although potentially daunting, ramping up preparedness has its silver lining. You can view it as an organisational stress test – one that can and should lead to improvements in your processes. In today's risk landscape, a company's degree of readiness to handle a cyber-crisis can also be a marker of competitive advantage and, ultimately, its survival.

“My message to boardrooms throughout New Zealand is to consider your cyber vulnerabilities as a key business risk and have a conversation about how you're going to address them as part of your risk management processes.

Strong cyber security practices will enable businesses to be productive, profitable and competitive. It's also important for the country's international reputation as a safe place to do business and store data.”

Amy Adams, New Zealand Communications Minister
10 December, 2015

IT threats and mitigations are the responsibility of the entire organisation



Executive level:

- Institute sound cybersecurity strategy
- Ensure quality information is received and assimilated
- Implement user security awareness programmes
- Enable strategy-based spending on security



Audit and risk:

- Ensure a thorough understanding and coverage of technology risks
- Conduct up-front due diligence to mitigate risks associated with third parties
- Address risks associated with operational (non-financial) systems
- Address basic IT audit issues



Legal:

- Track the evolving cyber-regulatory environment
- Monitor decisions made by regulators in response to cyber incidents
- Be aware of factors that can void cyber insurance



IT:

- Conduct forensic readiness assessments
- Be aware of the changing threat landscape and attack vectors
- Test incident response plans
- Implement effective monitoring processes
- Employ new strategies: cyber-attack simulations, gamification of security training and awareness sessions and security data analytics



Ethics & compliance

Managing the balance between trust and compliance can be the difference in retaining or losing top talent. In today's continuously evolving marketplace, having a strategy for aligning ethics and compliance with business risks will keep you on the path towards realising your opportunity



Aligning values and strategy with risks and responsibilities

Economic crime compliance risks are showing no sign of abating. That's hardly a surprise in a business environment characterised by growing globalisation and complexity in methodologies and areas of enforcement. Not only are the number of compliance risks increasing but so are the complexity of those risks and the number of regulators.

A risk-based approach to 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 for today's organisations. From that position of clarity, you can define your rules, roles, responsibilities and lines of defence and create a programme that mitigates those risks. This positions you for reaching your business goals and is the strategic focus of our survey.

In many industries and geographies, risks are not diminishing, and a short corporate memory can be dangerous. The deeper point is that while risks are ever-changing, the essence of a successful compliance programme is to foresee and address an evolving risk landscape.

A disconnect

Despite the growing emphasis on ethical values in corporate communications and the widespread adoption of business ethics and compliance programmes, our study suggests there is often a disconnect between the tone at the top and the reality on the ground (both behavioural and budgetary), leaving organisations vulnerable to compliance breakdowns.

The numbers point to a perception gap between what CEOs and boards believe and say and what's actually happening in the business. This is particularly true for middle managers, who remain the most likely to commit fraud. This is the group that our survey finds are more likely to feel that organisational values are not being clearly stated or that incentive programmes are not fair.

The true meaning of fit-for-purpose

To compete at the highest level, today's organisations need to be able to demonstrate that they are committed to embedding ethical behaviour throughout their operations as a key part of corporate strategy. Good policies, procedures and controls will not suffice: words need to be backed up by actions, and front-line staff need to have the tools that will help them to live the behaviours their leaders champion.

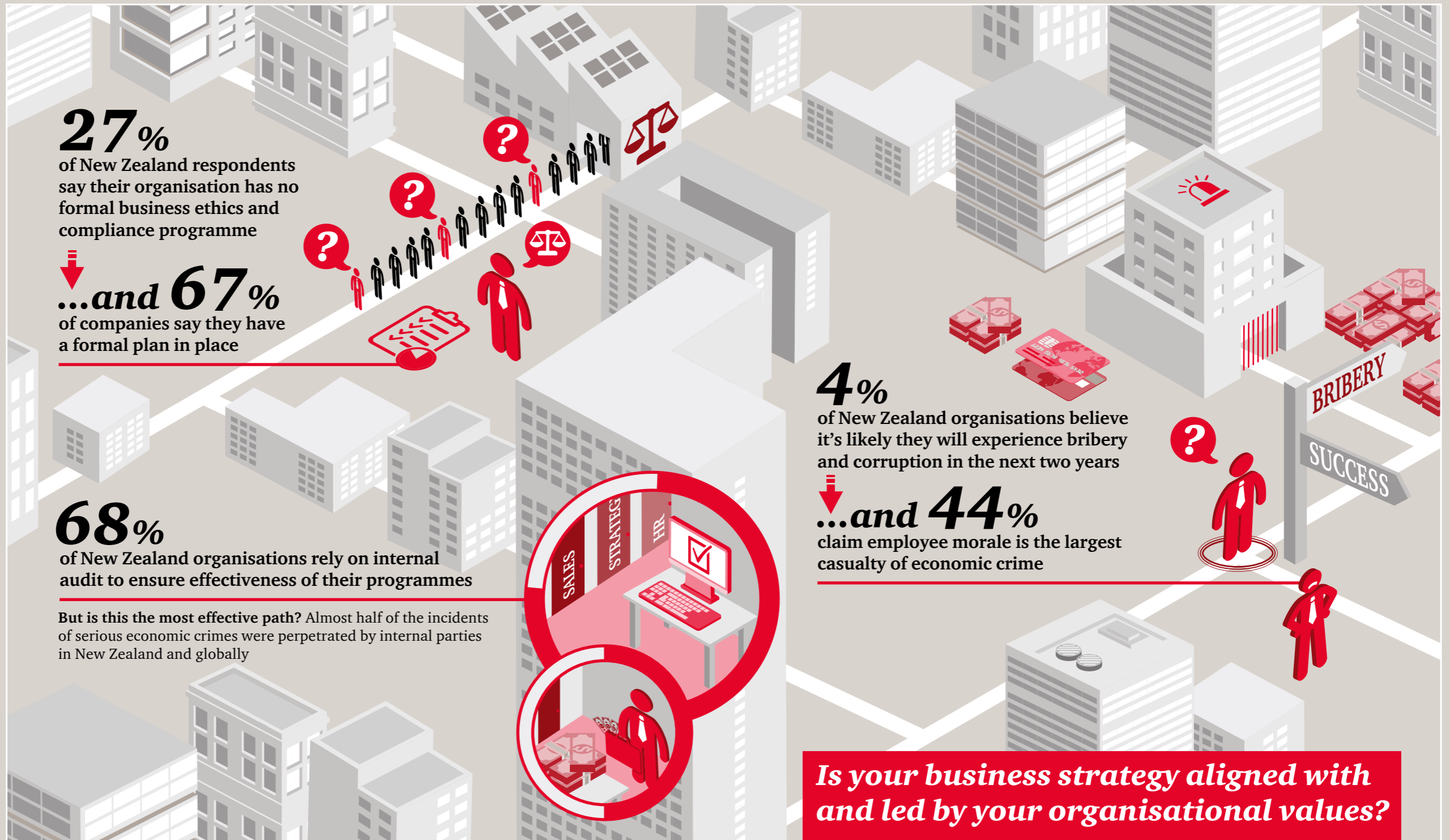
So how do the C-suite ensure that what they espouse is actually being put into practice by management? How is compliance being incentivised? How is it being measured?

There are four key areas of focus for enhancing the effectiveness of compliance programmes:

- **People and culture.** Maintaining a values-based programme, measuring and rewarding desired behaviours
- **Roles and responsibilities.** Ensuring they are correctly aligned with current risks
- **High-risk areas.** Better implementing and testing in high-risk markets and divisions
- **Technology.** Better use of detection and prevention tools, including big data analytics



In New Zealand responsible people want to work for responsible companies – ones who bring life to their ethical beliefs and 'walk the talk'



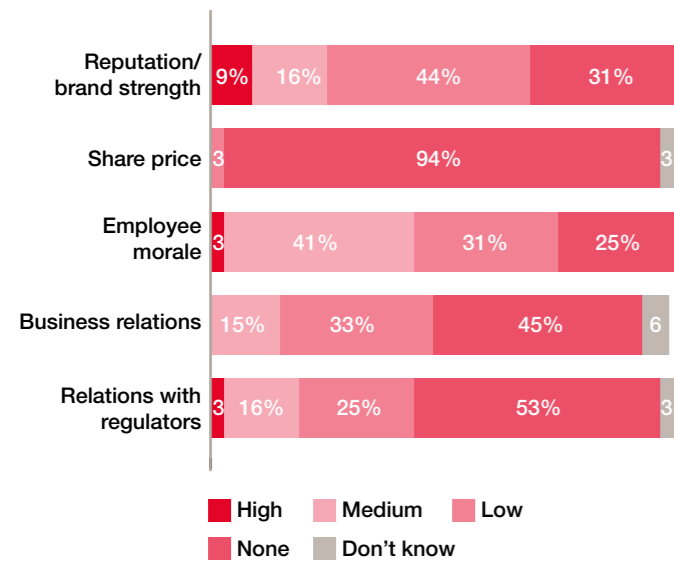


People & culture: your first line of defence

At the heart of any economic crime, irrespective of why it was committed, is a poor decision driven by human behaviour. That means not only instilling clear processes and principles for employees, but also creating a culture where compliance is hard-wired to values.

In New Zealand, the greatest organisational damage experienced as a result of economic crime was reflected in damaged employee morale, with 44 per cent citing a medium to high impact, and reputation, with 25 per cent. In both cases, the nature of how a business is perceived – from the inside as well as the outside – was the area of greatest concern. This underscores the key role played by appropriate values in a business.

Impact of economic crime in New Zealand



Source: New Zealand respondents

A values-based compliance programme is about attracting the best and the brightest to your organisation. Ethical people want to work for responsible companies – ones who not only are able to 'walk the talk' but who also align incentives and training with responsibilities and actions.

In a fast-changing world, a well-designed economic crime compliance programme – supported by a focus on supporting ethical behaviours – can offer a clear strategic benefit to the business. As such, it should include mechanisms to help motivate and reward your people, and to measure outcomes.

But to be effective, the compliance programme must comprise more than an updated code of conduct, a policy, and a few hours of training. Fundamentally, it must address the deep connection between values, behaviours and decision-making.

This approach endeavours to empower people with an underlying appreciation of how and why to make the right decisions, rather than just attempting to address or anticipate individual risks as they arise.

Recognising the typical dependence on cultural controls to identify fraud, the importance of these programmes should not be underestimated.

Mind and measure the (perception) gaps

Nearly all (91%) New Zealand respondents agreed that their organisation had clearly stated and had well understood organisational values. Globally, CEOs and CFOs expressed this particularly strongly, but our survey identified some areas where practice through the organisation ran behind senior managements' expectations.

Perception gaps

A persistent theme in the survey results is that of gaps in perception, which can lead to unwanted outcomes. These can be broken down into three basic categories:

- The gap between what the board believe and promote, and what people inside the organisation actually see, believe and do day to day.
- The gap between intentions and funding.
- The gap between senior management and middle managers in overseeing compliance.



Perceptions of business ethics and compliance

Organisational values are clearly stated and well understood



There is a code of conduct that covers key risk/policy areas



Ethical business conduct is a key component of our HR procedures



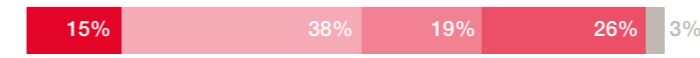
There are confidential channels for raising concerns



Senior leaders and managers convey the importance of ethical business conduct in all that they do



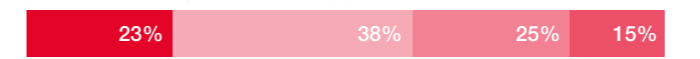
Training on the code of conduct (and supporting policies) is provided regularly



Irrespective of level, role, department or location, rewards are fair and consistent



Irrespective of level, role, department or location, disciplinary procedures and penalties are applied



Concerns can be raised confidentially, without fear of retaliation



Legend: Agree strongly (dark red), Agree (medium red), Neither agree nor disagree (light red), Disagree (very light red), Disagree strongly (grey)

Source: New Zealand respondents

This kind of gap – between what senior leaders think and say and what middle management perceive – can potentially create a vacuum within which, despite the best of intentions, unethical activities can spring.

Aligning roles and responsibilities: who's in charge here?

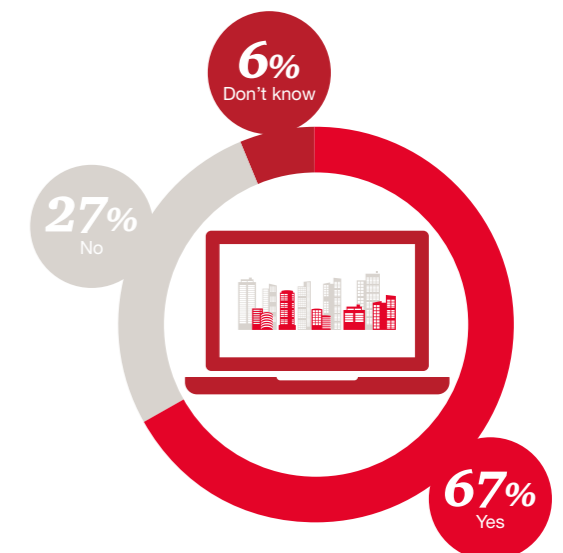
Our survey revealed that a significant number of New Zealand businesses have no formal compliance structure. (In some cases this may be due to the small scale of the companies.) Approximately one in four (27%) of all respondents told us they knew of no formal ethics and compliance programme in place in their companies.

Of the 67 per cent of organisations who do have a formal business ethics and compliance programme, responsibility for that programme is widely dispersed among roles.

The importance of being clear as to who is responsible for the different aspects of fraud control cannot be over emphasised.

Having a recognised code of conduct is important, but if employees do not know how to use it in their day-to-day decision-making this does little to mitigate compliance risks. The code and other policies need to be embedded through training, regular communications, reward and recognition of where good decisions are made – and disciplinary procedures where bad decisions are made.

New Zealand organisations which have a formal business ethics and compliance programme





Responsibility for business ethics and compliance programme

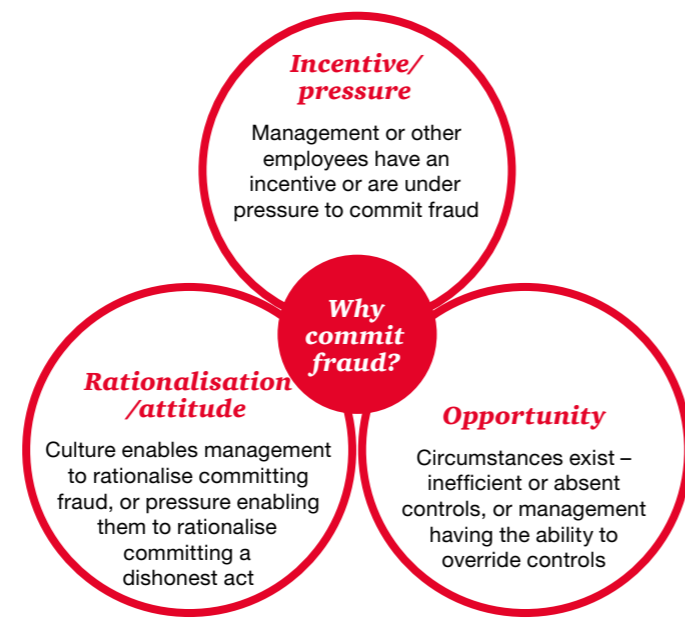


Source: New Zealand respondents

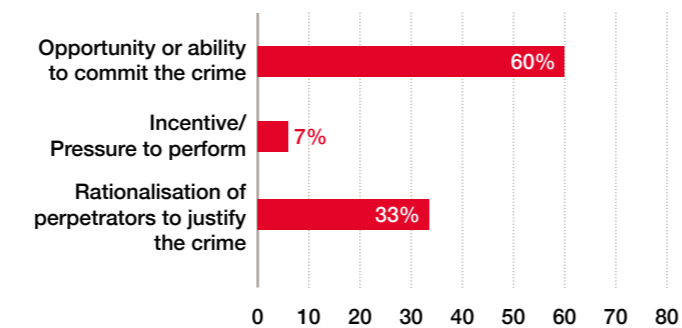
While smaller organisations (those with fewer than 1,000 employees) are less likely to have a formal business ethics and compliance programme, many of them face a similar risk landscape to larger organisations. This can pose a challenge for them in ensuring that they have an appropriate and proportionate programme in place.

Fraud – opportunities for the fraudster – and you

Six in 10 organisations believe that opportunity is the main driver of internal economic crime – far outweighing the other two elements of the fraud triangle, which are incentive/pressure to perform, and rationalisation of the crime.



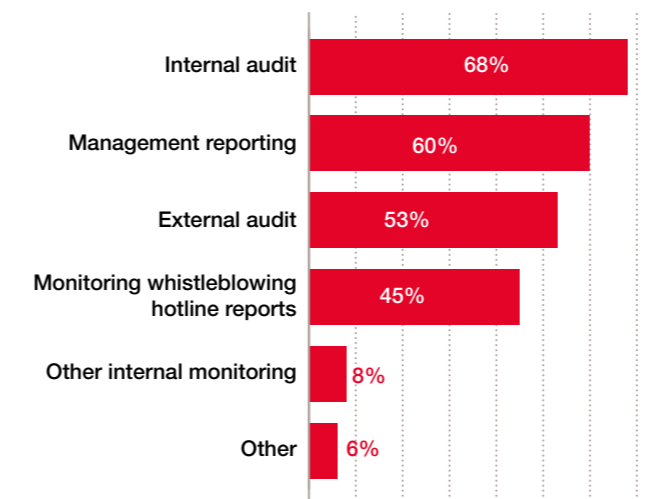
What factor do you feel has contributed the most to economic crime committed by internal actors?



Source: New Zealand respondents

So where is the best opportunity to prevent economic crime? A large majority favour stronger control environments. Nearly three quarters (68%) of New Zealand respondents told us they are relying on their internal audit (IA) function as part of their approach to assess the effectiveness of their compliance programmes.

Assessment of business ethics and compliance programmes



Source: New Zealand respondents

Experience shows, however, that internal audit – while an important piece of the framework for assessing a compliance programme’s effectiveness – is not a sufficient means of assuring compliance, due to the fact that its interventions are typically periodic and historical.

In fact, New Zealand detection rates for economic crimes by way of corporate controls such as internal audit, suspicious transaction reporting and the like have fallen dramatically to only 24 per cent (from 56% in 2014) whereas corporate culture controls (tip-offs and whistleblowers) remain high at 42 per cent (up from 37% in 2014). An unsettling 33 per cent of instances were identified by other factors, such as chance.

Because 42 per cent of all economic crimes are identified through tip-offs, a robust whistle-blowing service which meets the context and scale of the organisation is now a must have. Public sector organisations are required to align with the Protected Disclosures Act 2000 and many private sector businesses in New Zealand have voluntarily followed suit with independent whistleblower services.

Implementing in high-risk areas: the devil is in the details

While most respondents have undertaken fraud risk assessments, one in four have not done so in the last year. A simple fraud assessment and a review of your organisation's Fraud Control Framework – focusing on the prevention, detection and response to attacks on your 'crown jewels' – is a key step.

This is especially critical for organisations with operations overseas where bribery and corruption risk are considerably higher than in New Zealand. While appropriate training and communication costs money and time, it is nonetheless critical to the task of embedding the code of conduct across all business practices and locations – especially in geographic markets and divisions where risks of a breach are higher. This should include targeted training, consistent communication and management reporting. It should also include an understanding that country risks are not created equal (even across high-risk areas) – and that a sophisticated global compliance programme must be finely tuned to the specific realities on the ground.

We should put technology to better use

The local evidence suggests that technology is not doing its job to identify events of fraud, with only 24% of frauds unearthed by all forms of corporate control and only 6% uncovered by suspicious transaction reports. Data analytics tools are available enabling a better job to be done. Organisations need to improve their use of technology to protect key assets at risk.



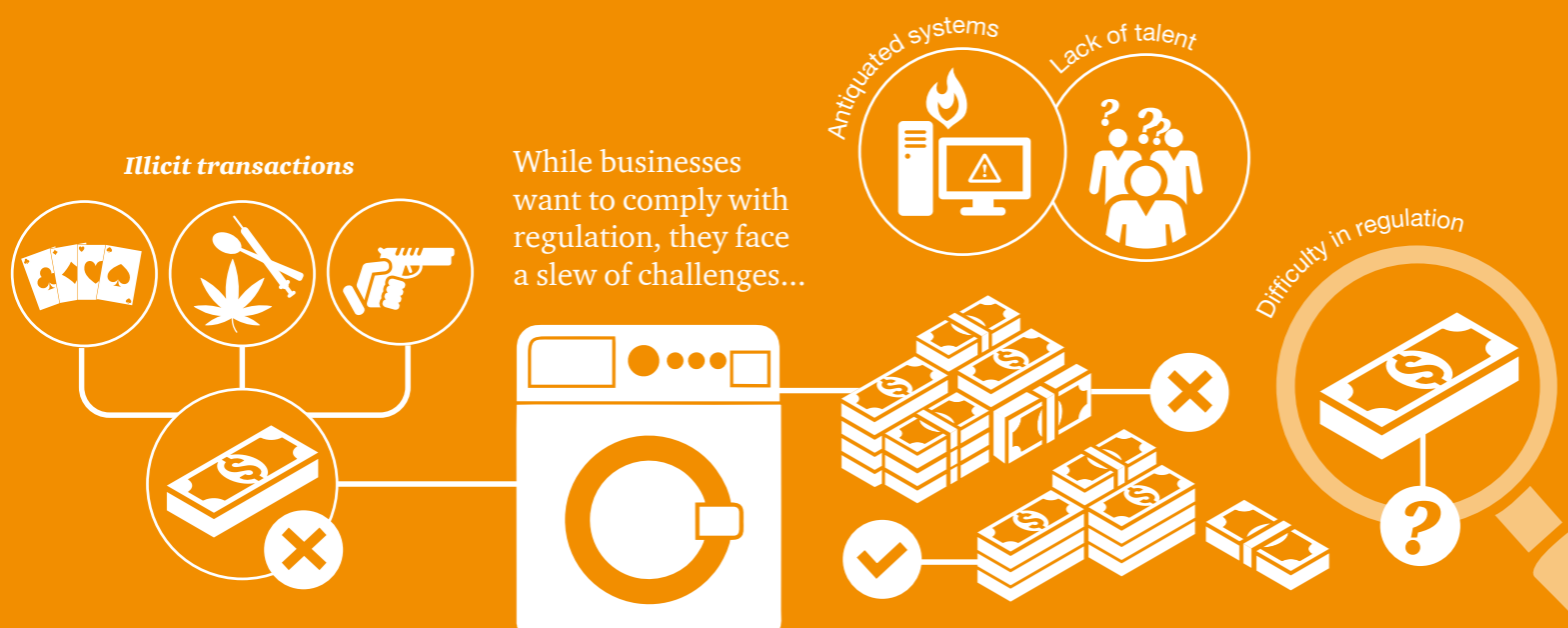
Anti-money laundering

Are you prepared to respond to the fast-changing regulatory environment?

New Zealand's anti-money laundering regime has been in operation for almost three years following the introduction of the Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act in 2013.

But more will come eventually: Phase Two of the Act will bring in many professional services including accountants, lawyers and real estate agents. What we do know is that the costs and time to fully comply are far greater than anticipated and that the when the scope is extended – as it has been in most other complying countries already – the costs and inconvenience to business and their customers will only grow.

At present the Act applies to financial institutions – banks, finance companies, brokers, remittance agents and the like – many of which are still struggling to be fully compliant. All of us will have been impacted at some level by the AML/CFT Act. For example, being asked to provide identification at the bank you've been with for years or producing a letter to confirm your address. A slight inconvenience, but the Act has had significant compliance complications and costs for financial institutions: some have struggled to find a bank to operate through, and some have closed up. Others have been required to contact all their existing customers and obtain identification, to set up expensive systems to monitor transactions, and then to query unusual transactions which may then be required to be reported to the Police.





Heightened regulatory standards are driving sharp increases in enforcement action across the globe

1 in 5 financial services respondents globally have experienced enforcement actions by a regulator

The pace of regulatory changes is also increasing

More than 25% of financial services firms have not conducted AML/CFT risk assessments across their global footprint or don't know if they have

33% of financial services respondents globally cite challenges with data quality

...only 50% of money laundering or terrorist financing incidents globally were detected by system alerts

...and 19% of global respondents claim that the ability to hire experienced staff is the biggest challenge to AML compliance

How would your organisation fare in the face of regulatory scrutiny?



The reputational and regulatory risk in New Zealand

Being associated with funds that have contributed to the financing of terrorism or linked to the 'legitimation' of criminal proceeds is a reputational and regulatory risk for financial entities. This is not a concern only for established companies but also for those who are hoping to establish themselves in New Zealand.

We have seen a marked increase in offshore financial entities seeking to establish a footprint in New Zealand. Most of those entities discover quite quickly that they are required to comply with New Zealand's AML legislation.

The Introduction of the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Act 2009 in New Zealand has seen AML not only climbing the political and regulatory agenda, but also increasingly on the agenda for the AML/CFT Act 'Reporting Entity' company boards and senior managers.

While reporting entities are prioritising their obligations, many of our clients have faced greater challenges than expected in implementing their AML/CFT procedures, policies and controls.

Many of New Zealand's reporting entities are part of global groups with AML experience in other jurisdictions. Adapting and modifying offshore AML programmes requires care and expertise and many New Zealand reporting entities have found themselves in breach of the AML/CFT Act, although compliant with their global requirements.

For example, practically implementing customer due diligence (CDD), to meet New Zealand's requirements has resulted in non-compliance across a range of entities. Assuming that the requirements or those of Australia, for example, will be satisfactory, is a mistake that can cost in terms of audit reporting and AML/CFT Supervisor intervention.

Documenting appropriate employee vetting and training has been another common area where incomplete compliance has put reporting entities at risk of supervisor intervention.

As reporting entities struggle with implementation, the finance sector has also been impacted by other increased compliance requirements. We have seen increased steps by the banking industry to address these issues by 'debanking'. This involves attempting to prevent riskier businesses from establishing or continuing banking relationships. An unintended consequence of this is to discourage the growth of innovative payment solutions and increase the costs of money making remittances for consumers. Furthermore, reporting entities who are at risk of being debanked struggle to secure banking arrangements, which can result in an increased use of less transparent payment channels.

While the implementation of the AML/CFT Act is going some way to combat money laundering and financing terrorism, reporting entities are facing significant challenges to operationalise the solutions.

Some New Zealand reporting entities have found themselves in breach of the AML/CFT Act, although compliant offshore.

New Zealand's AML/CFT regime is one of the world's newest. What can the global experience inform us on what is coming and what New Zealand businesses should be on the lookout for?

50%

Only half of money laundering (ML) or terrorist financing (TF) incidents in financial services respondents were detected by **system alerts**. Do the benefits of updating your legacy transaction monitoring system outweigh the costs? **Reporting entities in New Zealand are required to monitor transactions for suspicious activity. Most entities have automated systems to do this. The biggest challenge we see during our audits of reporting entities' AML/CFT programmes, is whether the triggers implemented are based on the risks identified, and confirming that the triggers actually work as expected.**

1 in 8

13 per cent of financial services respondents had been inspected and needed to address **significant issues**. Another 5 per cent were in a money-laundering remediation programme. Is your compliance programme vigilant enough? **We suggest that the New Zealand level of non-compliance is much higher. This is partly due to the newness of the regime, but also impacted by reliance on global AML programme.** The Financial Markets Authority took follow up action on 29 per cent of the audit reports it reviewed in its 2015 financial year.³

19%

The two biggest challenges to effective AML compliance cited by financial industry firms are the **pace of regulatory change** and the **lack of skilled staff** (each at 19%). Are you developing a programme that's adaptable to a changing risk landscape and increasing regulatory expectations? Are you hiring people with the right skills to support it? **All industry players in New Zealand are still learning and 'feeling their way' to varying degrees. We anticipate increased regulatory action against reporting entities in the future as expectations of compliance increase.**

14%

of financial services respondents have **not carried out money laundering or terrorist financing risk assessments** – of these, more than a third don't believe such assessments to be necessary. Should anti-money laundering programmes be your first line of defence in reducing these crimes? **To comply with the AML/CFT Act, reporting entities are required to complete a AML/CFT risk assessment prior to developing their AML/CFT programme.**

33%

of financial firms say the biggest challenge to their AML systems is **data quality**. Do you take steps to improve the quality of your customer data and related governance? **Reliance on agents to completed customer due diligence (CDD) is an area where many reporting entities are not compliant. The AML/CFT Act places strict liability on the reporting entity to ensure data obtained for CDD purposes is fully compliant.**

41%

Only four in 10 **non-financial services firms respondents are monitoring** for AML/CFT-specific red flags for their industry. Are you up to speed on the latest requirements you must meet? **Reporting entities must keep their AML/CFT risk assessment up-to-date. It is wrong to assume it's a static document.**



Money laundering destroys value

Money laundering facilitates economic crime and other illegal activity such as corruption, terrorism, tax evasion, and drug and human trafficking, by holding or transferring the funds necessary to commit these crimes. It can also seriously bruise an organisation's reputation – and its bottom line.

Global money-laundering transactions are estimated at 2 to 5 per cent of global GDP, or roughly \$1 trillion to \$2 trillion annually. Yet according to the United Nations Office on Drugs and Crime (UNODC), less than 1 per cent of global illicit financial flows are currently seized by authorities.

Given the recent increase in terrorist attacks, money laundering and terrorist financing are increasingly on the radar of governments across the globe. In the United States over the last few years alone, nearly a dozen global financial institutions have been assessed fines in the hundreds of millions to billions of dollars for money laundering and/or sanctions violations. There are strong indications that other countries will follow in substantive regulation and enforcement. In New Zealand, the AML/CFT supervisors are showing increased vigilance for reporting entities that are not compliant with the AML/CFT Act.

Any organisation that facilitates a financial transaction – including nonbank money transfer businesses such as digital or mobile payment services, life insurers, asset managers, retailers, and even tech-enabled ride-sharing services – is within the scope the AML/CFT Act. Many of these new participants are not compliant with the requirements they must meet.

The opportunity for companies is clear

Installing a robust, up-to-date AML compliance programme in accordance with New Zealand's AML/CFT Act – and embedding it effectively with your people, processes and technology – can yield multiple business benefits, not just with respect to AML efforts, but with other key compliance functions, such as anti-bribery, export sanctions, fraud monitoring and response, financial controls and investigations, potentially strengthening overall governance.

The rapid development of technology and e-commerce has seen increased innovative technologies and methods to launder 'dirty cash'. However, New Zealanders may be surprised to hear the traditional tried and true methods such as real estate and gold should not be overlooked.

With the continued development of e-commerce and mobile payment systems, methods to laundering money have become increasingly innovative and technically advanced.

The buying and selling of virtual currencies, such as Bitcoin, enables real money earned from criminal proceeds to be exchanged for virtual currencies and then later redeemed for real, or clean, money. While technology seeks to provide a clear audit trail, whether this information and the identity of the participants is available to AML regulators and auditors remains to be seen.

Online gaming enables money launderers to convert money from the real world into virtual goods and services or cash which can then be exchanged for cash in online games such as World of Warcraft. Less common methods but also on the rise are internet money mules whereby an employer will offer people jobs in which you can make a substantial income from working from home. However the job involves accepting money transfers into their accounts and then passing these funds to an account set up by the employer.

Despite these new and emerging methods, traditional money laundering methods are still used:

Real estate

With growing house prices, and increased demand for housing in New Zealand, criminal proceeds can be flushed through the housing markets through rapid off-market side transactions. With increases in sale prices occurring at such a high rate, gains can more easily be explained.

Gold

Off the back of the widespread implementation of AML/CFT regimes, one of the world's oldest luxury commodities is back in vogue. The fact that gold holds the same value and is readily accepted worldwide it can be used to settle debts with other criminals relatively easily with limited paper trails behind it.

Casinos

While you are still playing a game of odds, gambling is a consistent way to turn bad money into good. Criminals can turn up to a casino, use dirty money to place a bet and any winnings are clean. The sacrifice of losing half of the time is worth it to walk out of the casino with 100 per cent clean cash.

While reporting entities need to ensure they are staying abreast of new and emerging trends, traditional and reliable methods of money laundering are still with us.



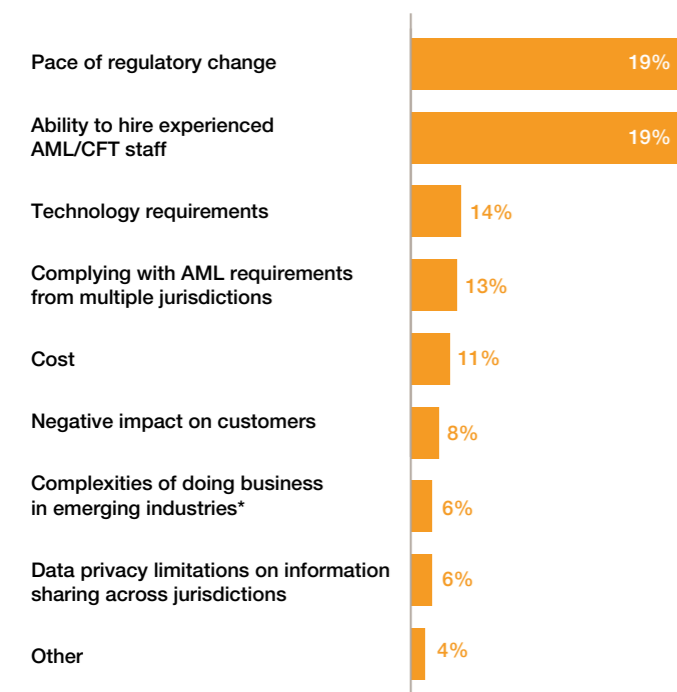


AML: The pace of regulatory change

Heightened regulatory standards are driving sharp increases in enforcement action.

Our survey shows that globally the level of enforcement of anti-money laundering and countering the financing of terrorism (CFT) measures has created challenges for even sophisticated financial institutions.

Which of the following do you see as the most significant challenge/issue in relation to complying with your local AML/CFT requirements?



* (such as legal marijuana, virtual currency, mobile wallet technology, etc)

Source: Global financial services respondents

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

Data privacy issues, too, have arisen, with certain jurisdictions setting more stringent standards than their counterparts in other countries on key business issues such as disclosure rules and access to customer data. These types of hurdles often make the management of AML risks across the enterprise extremely challenging.

In New Zealand, regulatory action to date has been limited to warnings and public notices. These sanctions are significant, but there is little doubt that in the future prosecutions and the risk of licences will be in store for non-compliant entities. As we note in the report, many reporting entities are non-compliant and supervisor tolerance will be limited.

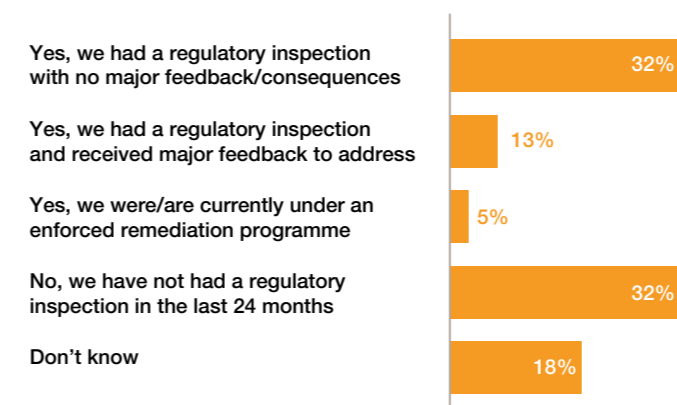
AML watchdogs and regulators

- The Financial Action Task Force on Money Laundering (FATF) is an inter-governmental policy-making and standard-setting body established by the Group of Seven in 1989. Its current mission is to promote policies to combat money laundering and the financing of terrorism by monitoring global AML and CFT trends, and setting international standards for combating these twin threats. FATF publishes its forty Recommendations – setting out a global minimum standard for an effective anti-money laundering system. Currently, 34 member countries including New Zealand have adopted the FATF Recommendations as part of their anti-money laundering regulation and legislation.
- The United Nations Security Council issues resolutions containing inter alia lists of persons against which sanctions have been imposed, such as known terrorist organisations. These lists are often used by participating governments to support measures against terrorist activity.
- The Office of Foreign Assets Control (OFAC) in the US administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers and those engaged in activities related to the proliferation of weapons of mass destruction.

Inspections and remediation are on the rise

Several financial groups have grown by acquisition, with some legal vehicles, businesses and markets not yet consolidated into group processes or standards. Many are also still struggling in the aftermath of regulatory actions or sanctions. All of these factors increase the risk profile for AML enforcements. Our survey indicates that 18 per cent of banks globally – a very significant number of financial institutions – have recently experienced enforcement actions by a regulator. The figure in New Zealand is already over 10 per cent for the banking sector.

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



Source: Global financial services respondents

Such enforcement actions, however, can be uneven. Most nation-states have some mechanism for AML inspections, but the degree of thoroughness of those inspections varies substantially. The United States and a few other developed countries have examination staff dedicated to AML and sanctions; in New Zealand these dedicated staff form part of the AML/CFT teams at the three supervisors – Reserve Bank of New Zealand, Financial Markets Authority and the Department of Internal Affairs.

FATF: A new focus on effectiveness

FATF has shifted its standard of evaluation of countrywide AML/CFT standards from technical compliance to effectiveness, where all organisations are measured by a similar yardstick.

This new focus on effectiveness will drive some developing countries to make changes in their enforcement practices, which will trickle down to institutions – and, in turn, given the global nature of AML initiatives, to other jurisdictions. It could also temporarily create a gap in perception of the meaning of 'effectiveness'.

Global regulation is the new normal

Strict compliance with the AML/CFT Act is required for New Zealand's reporting entities. However organisations should consider AML/CFT matters as being globally regulated. There are three primary reasons for this:

- FATF sets international standards for AML/CFT risk management and enforcement. As such it forms the basis for national regulations – and the obligations of banks and other regulated institutions.
- OFAC, along with other national treasuries such as Her Majesty's Treasury (HMT), administer economic sanctions programmes – and thus by design are focused on the movement of goods, services and funds overseas.
- It is almost impossible for financial institutions, in the course of doing business, to avoid the laws of the jurisdictions administering major global currencies such as the US Dollar, the British Pound and the Euro. The mere act, for instance, of clearing a single transaction in the US – or even of contacting a person in the US by telephone or email – is enough to establish the legal nexus and clear the way for prosecutions in the US.



What does this all mean for New Zealand reporting entities?

With the globalisation of AML/CFT standards, it's important to remember that while you are only as strong as your weakest link, from a compliance point of view you may be judged by the highest international standards. Here are three action points to consider:

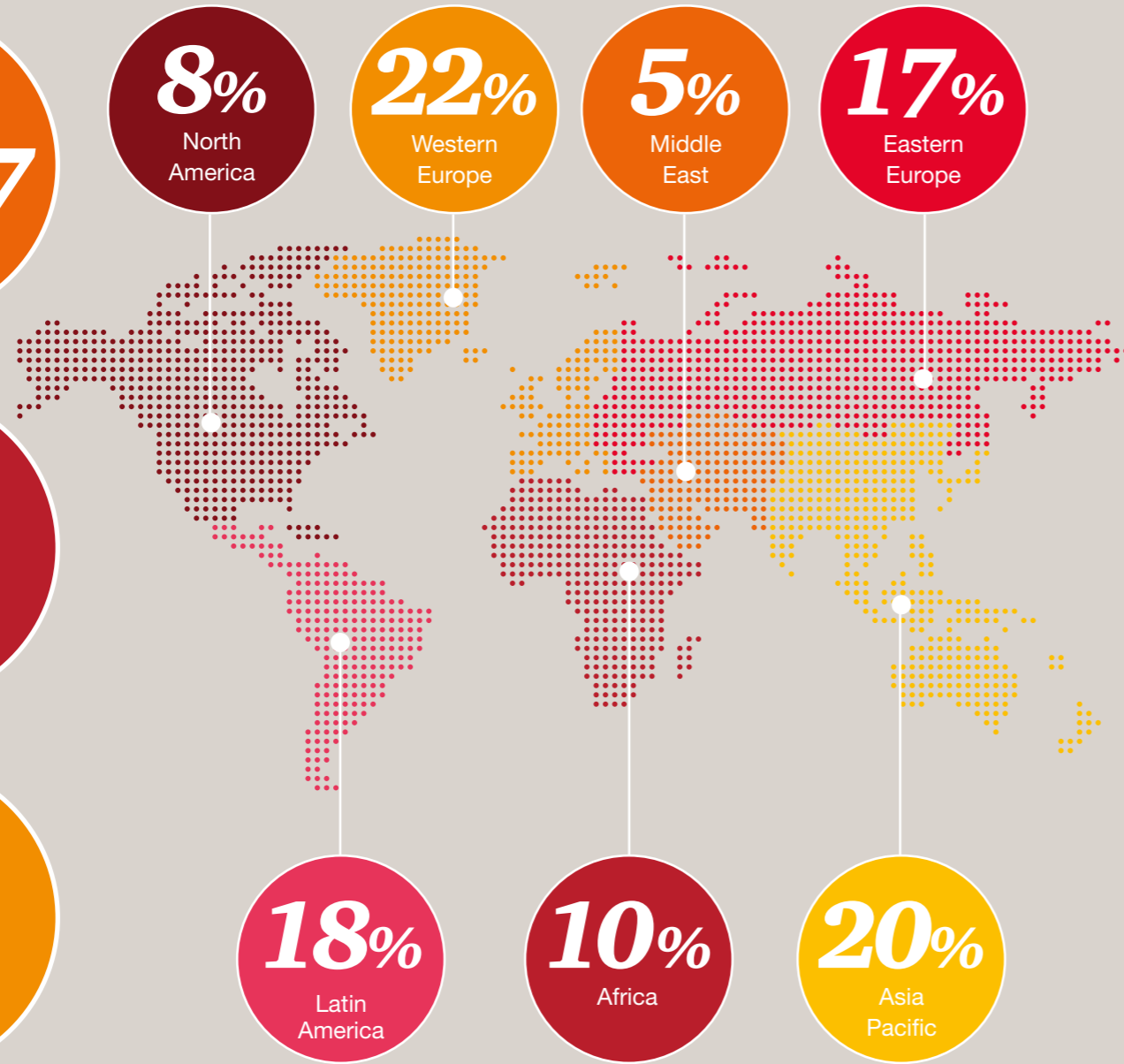
- 1. Keep your finger on the regulatory pulse.** Forward-thinking organisations are looking beyond mechanical compliance with today's laws – and looking ahead to structure themselves to comply with upcoming legislative trends. Having a viable function within the organisation that keeps track of pending regulations in this area is critical.
- 2. Lead the pack; don't follow.** Being in the middle of the pack exposes you to the risk of falling behind the regulatory curve. Being strategically nimble and innovative can help you stay on top of the regulatory changes.
- 3. Learn from other reporting entities' mistakes.** Few organisations are known to actively investigate the root cause of significant issues identified by regulators. Remediation often serves as a quick solution to address regulatory findings – yet the cost of remediating breaches often far outweighs the penalties imposed by regulators. Since many transactions have a multinational financial component, it is good practice to default to the highest global standard of compliance whenever possible, and to undergo more rigorous AML/CFT self-assessments. Establish enterprise-wide requirements to ensure consistency across geographies, channels and products.

Global participation statistics

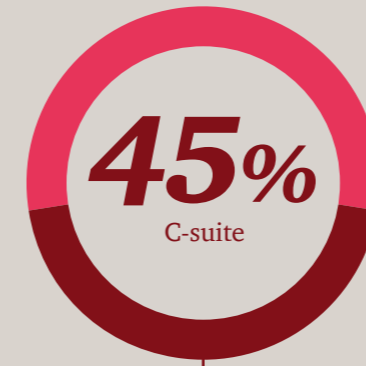
Participation statistics



Participation by region



Respondents



70%

of respondents were in executive management, finance, audit, compliance or risk management

54%

of respondents employed by organisations with more than 1,000 employees, with

48%

of these participants having more than 10,000 employees

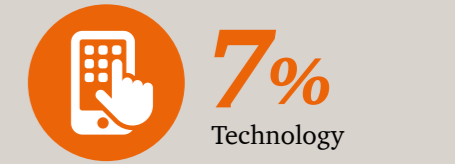
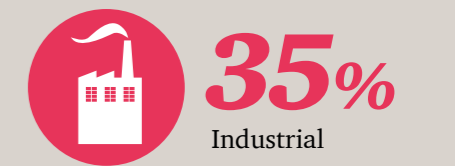
37%

of the survey population represented publicly traded companies, and

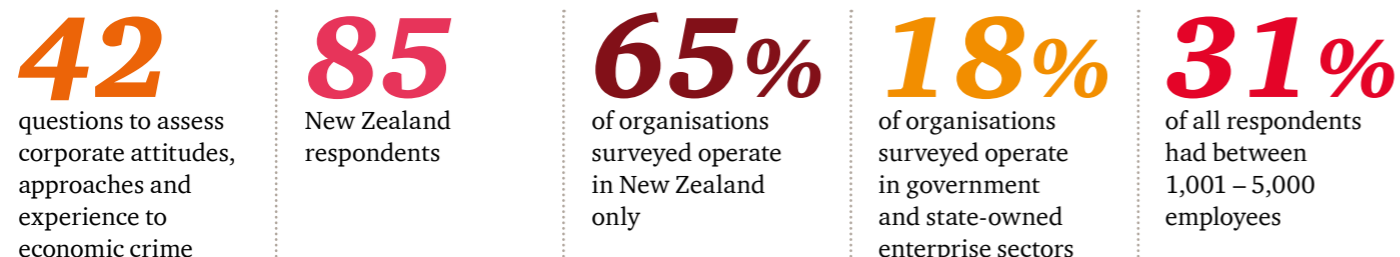
59%

of respondents were from multinational organisations

Industry sectors



New Zealand participation statistics



How many employees does your organisation have?

Up to 100 employees	18%
101 to 500 employees	24%
501 to 1,000 employees	14%
1,001 to 5,000 employees	31%
5,001 to 10,000 employees	5%
More than 10,000 employees	8%
Don't know	1%

What industry does your organisation operate in?

Communications	1%
Energy, utilities and mining	12%
Engineering and construction	4%
Financial services	16%
Government/state owned enterprises	18%
Manufacturing	5%
Insurance	8%
Pharmaceuticals and life sciences	1%
Professional services	4%
Retail and consumer	8%
Technology	1%
Transportation and logistics	2%
Agriculture	5%
Education	5%
Healthcare	6%
Other industry/business	5%

In how many countries does your organisation have offices?

One only	65%
2 to 10	26%
11 to 25	1%
26 to 50	4%
51 to 100	2%
More than 100	2%

Which of the options below best describes your organisation's ownership structure?

Publicly traded company	26%
Privately owned	25%
Government/state-owned enterprise	25%
Other	25%

Appendix

Data resources

Purpose of the 2016 survey

The aim of our survey was to assess corporate attitudes, approaches and experiences to economic crime in the current economic environment, and particularly to understand whether the incidents of cybercrime-related fraud is becoming more prevalent in recent years, the prevalence of other forms of economic crime including asset misappropriation, bribery/corruption, money laundering and anti-competition, what types of fraud are most common, the impact of ethics and compliance and the state of AML compliance.

Terminology

Statistics referred to in this report generally refer to New Zealand, unless otherwise stated.

Looking for more data?

The crime survey website www.pwc.com/crimesurvey has been designed to be an extension of the survey with many exciting and useful resources for readers wishing to delve deeper into the data, including:

- Survey methodology
- Terminology
- Comparative country counts
- Additional information regarding the nature of participants

In addition, this year's survey data has been loaded onto an innovative tool referred to as the Global Data Explorer which will allow visitors to the site the ability to customise their analysis of the data for their specific needs.

About PwC Forensic Services

The Forensic Services group of PwC's global network of firms provides our clients with the full range of investigative response to fraud and other forms of economic crime. We also assist our clients in undertaking prevention and detection measures to better protect themselves from fraud.

Your PwC New Zealand Forensics Team also has specialists with expertise in cybercrime, electronic discovery and anti-money laundering compliance.

Contacts



Eric Lucas
Partner
Forensic Services
+64 9 355 8647
eric.lucas@nz.pwc.com



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



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

pwc.co.nz/crimesurvey