

Economic crime: What you don't know can hurt you



33%

One third of New Zealand organisations report being victims of economic crime.

40%

Four in 10 New Zealand CEOs report being concerned by cyber threats, including the lack of data security.

Five

'Big fraud threats' most commonly affecting New Zealand organisations.

Contents

1 Economic crime: What you don't know can hurt you

3 What do the survey results tell us?

4 Types of fraud reported

5 Who is most affected?

6 Future predictions

7 Under the eye of enforcement

8 Are New Zealand companies aware of their obligations?

11 Combating bribery and corruption

13 High impact economic crimes

14 Procurement fraud by industry

15 Asset misappropriation

15 Accounting fraud: The connected threat

16 Cybercrime: The risks of a networked world

22 Identifying the fraudster

30 Appendix

Welcome to our New Zealand supplement to PwC's 2014 Global Economic Crime Survey.

It will surprise few to learn that economic crime – such as fraud, corruption, cybercrime, IP infringement or accounting fraud – continues to be a major concern for New Zealand organisations of all sizes, across all regions and in virtually every sector.

Indeed, one third of New Zealand respondents to this year's survey reported their workplaces being victimised by economic crime in the past two years. It's an alarming finding and a reminder to all organisations to remain vigilant to the threats they face.

This is just one headline from the New Zealand supplement to our 2014 Global Economic Crime Survey: one of the broadest and most comprehensive economic crime surveys we have ever conducted, with 82 local respondents and over 5,000 global respondents contributing from every corner of the world.

But the real story is greater than economic crime persisting: it's also about economic crime threatening your business processes, eroding the integrity of your employees, and tarnishing your reputation. Which is why this year's report is focused on how and where it may be affecting you – so you can address the issue from both a preventive and a strategic perspective.

We thank all those who took the time to add their voice to this global study, in order to give us a better understanding of the fraud threats we face in New Zealand. Your contribution is invaluable.

Our report also focuses on enforcement activity; which touches on New Zealand's new anti-money laundering regime and high impact economic crimes, such as procurement fraud and cybercrime.


We hope our survey findings and analysis will serve your stakeholders well – including the Board, management, staff, suppliers, business partners and regulators – as both a useful reference point in an endless campaign and a strategic tool in your business arsenal in the year ahead.

Our senior forensics team of Stephen Drain, Campbell McKenzie and I would be pleased to discuss our findings with you personally, how they relate to your organisation, and what you can do to better protect your business.

Best regards,



Eric Lucas
Forensic Services Partner
PwC New Zealand



Economic crime continues to be a major concern for New Zealand organisations.

One third of New Zealand respondents report their workplaces were victimised by economic crime.

Economic crime: What you don't know can hurt you

Economic crimes fundamentally threaten the basic processes common to all businesses – paying and collecting, buying and selling, hiring and firing. Since close interaction with others is the foundation upon which virtually every business function is built, all organisations are exposed to various types of economic crime.

This is as true for New Zealand as it is anywhere in the world.

While New Zealand business confidence is high and the economic outlook looks bright, we found fraud continues to hit New Zealand companies in the pocket – and while it can be hard to measure the cost of goods falling off the back of trucks, kickbacks, the theft of intellectual property and ideas – we know that financial costs are far from the only or most costly concern.

For the first time this year, we asked respondents about procurement fraud, reported by 19% of New Zealand organisations affected by economic crime. Procurement fraud is seen as a double threat, victimising businesses both in their acquisition of goods and services and in their efforts to compete for new opportunities.

With the Canterbury rebuild, increasing trade with emerging markets, rapid urbanisation - and our digital capabilities eliminating the tyranny of distance our businesses have faced for so long - new threats have arisen from fraudsters increasingly turning to innovative schemes and technology to assist their criminal activities.

These risks continue to evolve, and like a virus, economic crime adapts to the trends.

We must remain alert to the threats we face, particularly in this environment where we can expect investment activity to accelerate.

While the survey suggests New Zealand ranks lower for economic crime than many other countries, we must ask whether our organisations are adequately monitoring and aware of fraud and security breaches, or simply not reporting them.

For example, global respondents told us around a quarter have been a victim of cybercrime compared to New Zealand's 11%. Significantly, our respondents expect cybercrime to be double from current reported levels to 22%, over the next two years.

Furthermore, being a systemic problem, cybercrime's direct economic impact can be exceeded by the effect on employee morale, brand and reputation.

Pleasingly, the results of our Annual Global CEO Survey show New Zealand business leaders are beginning to take the threat of cybercrime seriously, with four in 10 worried about cyber threats and the lack of data security. Cyber worries are moving up the threat radar and on the minds of the c-suite.

With anti-money laundering legislation coming into effect in 2013, respondents also reported high awareness of the legislation (82%), and a similar number reported they were aware of the requirements to be fully compliant.

As trade with Asia increases, New Zealand businesses are increasingly exposed to countries which may have higher levels of corruption. There are significant risks for New Zealand entities in engaging in facilitation payments which seek to by-pass official processes or transparent contractual arrangements.

Encouragingly, the survey found 71% of New Zealand respondents have a whistleblowing mechanism, with 37% of crime detected through tip-offs. While corporate controls are responsible for detecting 56% of crimes.

Economic crime in New Zealand

What you need to know

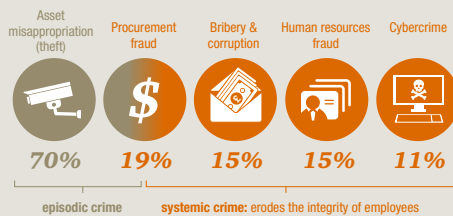
Economic crime continues to be a major concern for organisations of all sizes, across all regions and in virtually every sector. One in three New Zealand organisations reports being hit by economic crime.

33%

Financial losses are not the only concern: the true cost of fraud to reputation, employee morale and external relationships can be long lasting.

Most commonly reported types of economic crime

Five types of frauds are consistently reported – asset misappropriation, procurement fraud, bribery and corruption, human resources fraud and cybercrime.



The New Zealand c-suite gets the message

How **concerned** are you about the following potential business threats to your organisation?

43%

A lack of trust in business

Cyber threats including lack of data security

40%

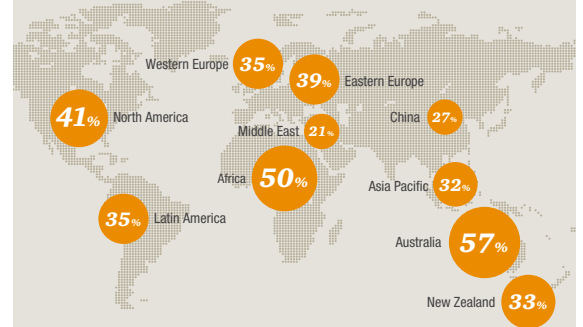
31%

Inability to protect intellectual property

New Zealand data from PwC's 17th Annual Global CEO Survey

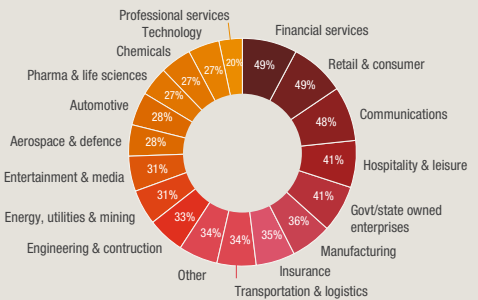
Where does economic crime occur?

Economic crime is a pervasive global threat. The highest levels of economic crime are consistently reported by respondents in Africa (50%) and North America (41%).



Which industries are at risk? A global outlook

By industry, economic crime is most commonly reported in the financial services, retail and consumer, and communications sectors. Nearly 50% of respondents in each said they had been crime victims.



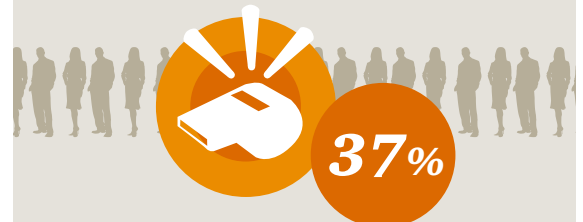
Processes under threat

Economic crimes threaten the basic processes common to all businesses – paying and collecting, buying and selling, growing and expanding, sourcing and supply chain.



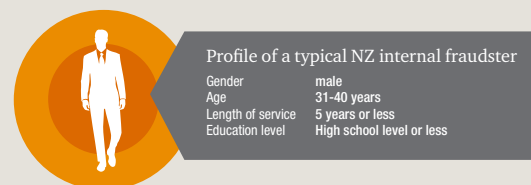
To catch a thief

Tip-offs, including whistleblowing, detect 37% of economic crimes in New Zealand.



Know your enemy

Businesses face threats from both internal and external sources and multiple angles. 70% of New Zealand organisations say the main fraud threat comes internally.



The internal threat has the greatest impact when senior managers are involved.

What do the survey results tell us?

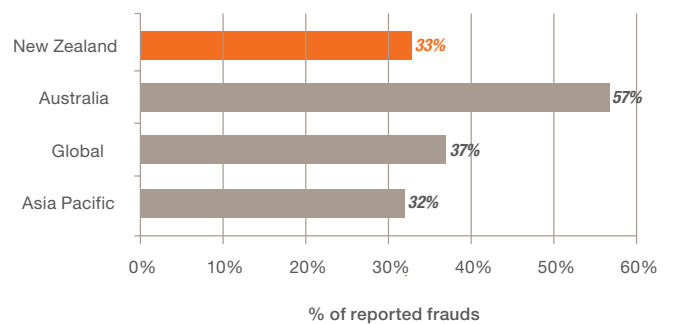
Of the 82 New Zealand respondents, 33% have experienced some form of economic crime during the survey period.

This ranks New Zealand 45th out of more than 95 countries that took part in the survey, and places us slightly below the global average of 37%, and significantly below our neighbours Australia (57%).

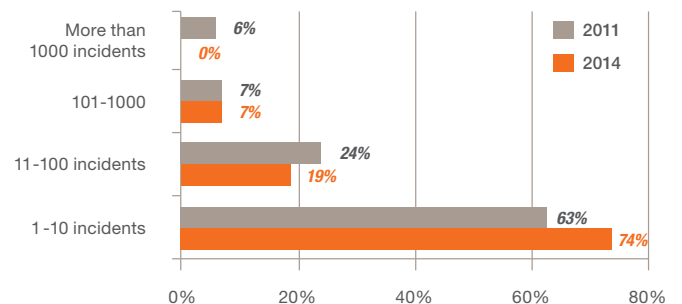
While the number of occurrences of economic crime appear to be decreasing in New Zealand, so too are the total number of incidents experienced. Over 74% of respondents said they had experienced less than 10 incidents over the survey period (2011: 63%). What's even more encouraging from a New Zealand perspective is that none of our respondents suffered more than 1,000 incidents (a decrease of 6.5% from 2011).

These findings are again consistent with New Zealand's image as one of the least corrupt countries in the world, and reflect Transparency International's 2013 Corruption Perception Index (where New Zealand again is perceived to have the lowest level of public sector corruption in the world).

Percentage of organisations experiencing fraud



Number of incidents of economic crime suffered by New Zealand organisations



New Zealand ranks

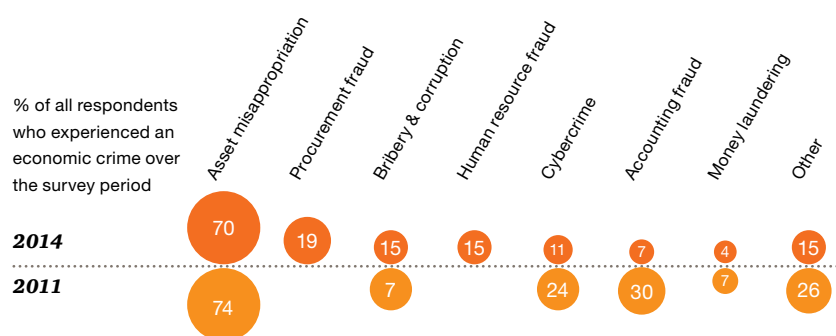
45th

out of more than 95 countries for reported incidents of fraud

Types of fraud reported

Consistent with last year's survey, our New Zealand findings show asset misappropriation is the most reported type of economic fraud (70%).

Types of fraud reported



Consistent with the global trend is an increase in the number of respondents suffering from incidents of bribery and corruption, with 15% of New Zealand respondents reporting their organisations have been a victim of this type of fraud. This is potentially linked to an increase in global awareness and is consistent with the findings from our 2014 Annual Global CEO Survey report, in which more than half of c-suite executives say they are concerned or extremely concerned by bribery and corruption.

Additionally, cybercrime continues to be an issue for New Zealand companies, with 11% of those who suffered some form of economic crime being the victims of a cybercrime. Also, it is highly likely that a number of respondents who have been victims of a cyber attack may not have an awareness of the crime. Unfortunately, far too often companies do not realise the true economic impact of a cyber attack until long after an incident has occurred.

Having included procurement fraud as a distinct category in this year's survey, it immediately registered as the second most reported type of fraud in New Zealand (19%). One likely reason, is the fact that New Zealand is in a period of growth due to the Canterbury rebuild following the earthquakes, and also has significant construction activity in Auckland, driven by immigration.

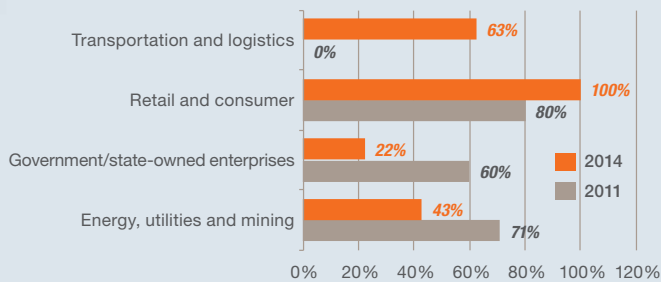
Globally, the high incidence of procurement fraud is likely driven by two distinct characteristics of today's economic environment. Firstly, business entities are becoming more interconnected, whether it be in outsourcing elements of the value chain, purchasing of materials or an increased reliance on suppliers: this is also consistent with the New Zealand findings of our 2014 Annual Global CEO Survey. Secondly, one of the effects from the recent global economic crisis is that companies have, and in some cases still are, replacing permanent in-house positions with more dispensable and scalable outside resources, with companies more willing to outsource non-core related tasks and in some instances even core tasks.

Interestingly, another distinct category that was added to this year's survey was HR fraud, which ranked joint third overall (15%) in terms of the types of fraud suffered. This is compared with a global ranking of sixth.

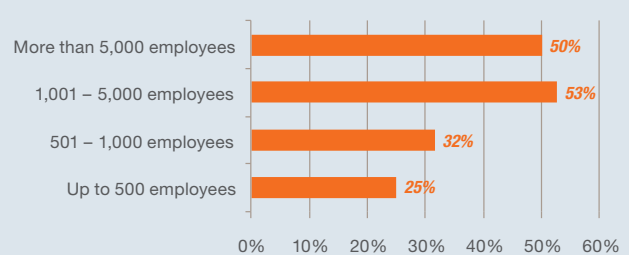
New Zealand respondents in 2014 reported 'other' economic crimes as insurance fraud, loan fraud and credit card fraud.

Who is most affected?

New Zealand industries experiencing economic crime



Reported frauds based on organisation size in New Zealand



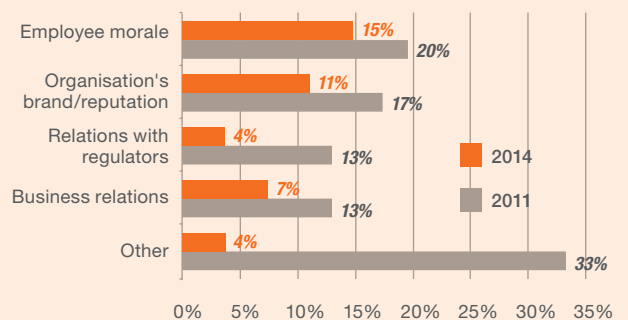
Estimating the damage

Often, organisations do not fully appreciate the true financial impact of an economic crime until after it has occurred. Although in New Zealand, our survey findings indicate the financial impact of economic crime declined for this survey period, global trends indicate the impacts of economic crime continue to be an increasingly costly issue.

However, financial loss is not the only concern that companies face. We also asked New Zealand organisations about the ‘collateral’ damage to their business operations, including questions related to employee morale, brand/reputation, business relations and relationships with regulators.

Of those who had experienced fraud, 15% reported significant damage to employee morale (2011: 20%), 11% significant damage to reputation/brand (2011: 17%), 7% significant damage to business relations (2011: 13%) and 4% significant damage to relations with regulators (2011: 13%).

Collateral damage associated with economic crime in New Zealand



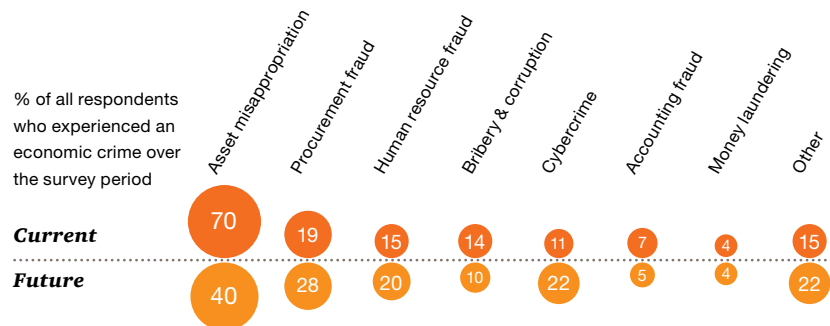
While the survey results may indicate that ‘collateral’ damage may be declining in New Zealand, it is imperative to remember the true cost of a fraud incident can be long lasting. While it’s difficult to quantify these kinds of losses in strictly financial terms, one fact is crystal clear: if fraud affects hiring, retention, the ability to work with vendors, customers, and reputation, the impact will be felt all over the income statement – even if it isn’t labelled as ‘fraud’.

Fortunately, top management appear to understand this: more than four out of 10 New Zealand business leaders in our 2014 Annual Global CEO Survey see a ‘lack of trust in business’ as a key marketplace issue, with significant majorities recognising that business has a wider role to play in society than just building shareholder value (71%).

Future predictions

In addition to looking at economic crime suffered in the past, we also asked respondents to look forward and tell us which frauds they thought would pose the highest risks to their organisations over the next 24 months.

Types of fraud predicted in New Zealand over the next 24 months



Our findings show that New Zealand companies are predicting occurrences of economic crime, as well as the total number of reported incidents, to persist over the next 24 months. Yet, there is a strongly predicted shift in the types of economic crime expected to impact organisations.

We can see New Zealand companies remain very cautious and predict they will experience more economic crime in areas such as procurement fraud and cybercrime.

We also note that occurrences of bribery and corruption are predicted to drop back, close to 2011 levels, while asset misappropriation is also predicted to drop from the 70% reported this year to approximately 40% over the next 24 months.



Under the eye of enforcement

Long reaching effects

Some types of economic crimes attract significantly more attention from government enforcement agencies than others. These types of economic crimes – i.e. money laundering, bribery and corruption and anti-competitive behaviour – arise from the failure of businesses to adhere to the expected code of business conduct established by countries around the world.

Each of these crimes are subject to government enforcement by the relevant authorities and are subject to increasingly stringent standards, enforcement and harsh penalties. In an interconnected world, these types of economic crimes pose unique threats to organisations.

Violations of government legislation, such as the recent Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT Act), can lead to substantial fines and have long lasting reputational effects for organisations.

Moreover, such violations may be indicative of larger organisational issues, such as weak internal controls or a lack of an appropriate tone at the top. This in turn can have a substantive knock-on effect for organisations, including reputational harm and financial loss, as well as issues related to talent retention and costly disruptions to business plans.

In fact, the findings from our survey indicate that across all three government enforcement-related frauds, respondents cited reputational risk as having the greatest impact on their business operations by a significant margin.

Money laundering: A special concern for financial services

Financial services companies report significant risk from an entirely different fraud than most other industries – money laundering. Money laundering represents a risk to financial institutions if they fail to have appropriate systems to deter, detect and report it.

Defined in our survey as actions intended to legitimise the proceeds of crime by disguising their true origin, the crime of money laundering exposes financial institutions in two ways:

1. Through access to laundered money provided to potential criminals.
2. Through the banking functions (e.g. bank accounts, loans, etc.) which fraudsters use to disguise funds.

What is the AML/CFT Act?

The AML/CFT Act was implemented as part of New Zealand's requirements to meet its international obligations. The Financial Action Task Force (FATF), an international body of which New Zealand is a member, has a requirement to have appropriate legislation in place to minimise the risk of money laundering. The legislation helps to reduce criminal activity in New Zealand by ensuring the illegitimate proceeds of such crimes are not put through the financial system (e.g. deposited to a bank account, etc) to disguise the true nature of these funds.

Under the Act, reporting entities (primarily financial organisations) have certain obligations. These obligations include the appointment of an AML compliance officer, undertaking a risk assessment, and based on the results of the risk assessment, developing a programme to comply with the requirements of the Act. Reporting entities also need to have their programme audited every two years to ensure continued compliance.

At its core, reporting entities will need relevant policies, processes and controls related to customer due diligence and account monitoring. This means financial institutions will need to ensure they have the appropriate rigour when it comes to their on-boarding process, specifically in relation to the identification and verification of new customers or if facilitating an 'occasional (one off) transaction'.

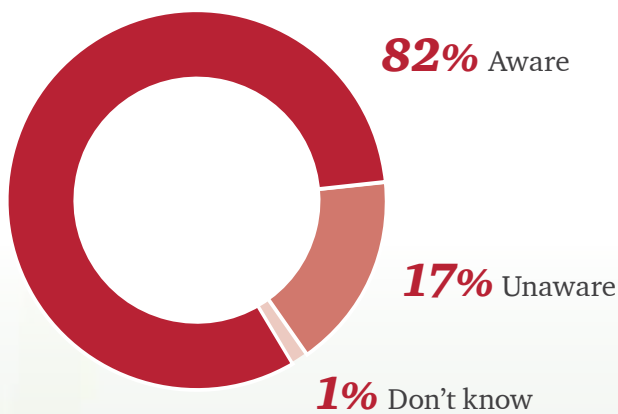
Under the Act, reporting entities are also required to have appropriate systems in place for reporting suspicious transactions to the New Zealand Police Financial Intelligence Unit (FIU).

Are New Zealand companies aware of their obligations?

In our survey, we asked respondents if they were aware that new anti-money laundering legislation had been enacted in New Zealand. Eighty-two percent of New Zealand respondents reported they were aware of the new legislation, and 81% also reported they were aware of their requirement to be fully compliant by 30 June 2013.

Penalties for non-compliance can be severe and a corporate body can incur a fine of up to \$5 million, as well as suffering substantial reputational damage in the market. For individuals, penalties can include imprisonment of up to two years and a fine of up to \$300,000.

Respondents' awareness of the AML/CFT Act enactment



Consider the difficulty faced by an international financial institution managing its operations in a variety of cultural and legal environments, yet subject to the stringent legal standards of a developed Western economy. For example, it must train tellers how to identify and report what might be 'suspicious transactions' – because of their amount, currency, the frequency of deposit, identity of the depositor, or unexplained nature of the business.

The institution may be operating within a culture known for violence or intimidation towards uncooperative individuals, for deference to the demands of the wealthy, or one in which corruption is commonplace. It could be operating in an environment where the relatively large difference between the economic circumstances of customers, relative to bank employees, allows for gifts or threats to pave the way for inappropriate use of its facilities by those charged with conducting transactions, approving transactions or reporting issues.



Sophisticated threats

Recently, a new form of money laundering threat has developed: alternative payment networks using 'virtual' currencies (e.g. Bitcoin). While the transactions on these sites may be 'virtual', they are backed by actual deposits in financial institutions around the world. Identifying such tainted funds is yet another challenge to bank compliance and operating systems.

So, operating in environments that pose a systemic threat of money laundering to the business processes of financial institutions is a unique challenge. Not only are money laundering schemes numerous and sophisticated, but they create a potentially significant tension between the equally laudable goals of acquiring and serving profitable customers and operating a wholly compliant institution across multiple jurisdictions.

Bribery and corruption: Are the c-suite getting the message?

While it is not the most common form of crime reported, of all the types of fraud covered in our survey, bribery and corruption may pose the greatest threat to businesses because of the number of business processes it threatens. Sales, marketing, distribution, payments, international expansion, expense reimbursement, tax compliance, and facilities operations are all vulnerable processes.

While New Zealand consistently ranks among the least corrupt nations in the world, our survey results indicate the number of reported occurrences of bribery and corruption is increasing. This year's results show that of the New Zealand respondents who have reported an economic crime, 15% have experienced bribery and corruption during the survey period (11%: 2011). This compares to a global average of 27% and is broadly in-line with the global trend, where occurrences of bribery and corruption have increased by 3% on average.

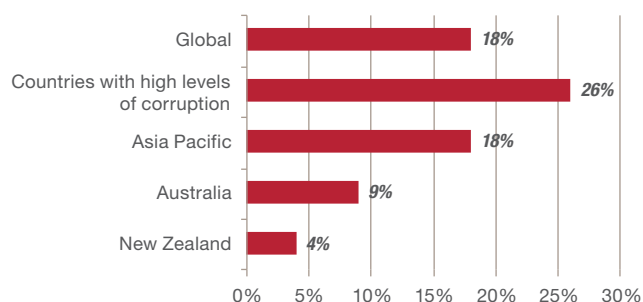
When such a crime threatens a company in so many ways, it deserves CEO attention. The findings from our 2014 Annual Global CEO survey show that over half of global CEOs now are either somewhat concerned or very concerned with the risks associated with bribery and corruption.

In New Zealand, the results are somewhat different; only 15% of our New Zealand CEOs indicated that risks associated with bribery and corruption are concerns for their organisations.

This is potentially linked to New Zealand's already good reputation for transparency and honesty. However, as the findings from our economic crime survey indicate, New Zealand CEOs should be more cognisant when it comes to considering the risks associated with this type of economic crime. Not only are the number of reported occurrences increasing, but of the three economic crimes falling under government enforcement, almost half of our survey respondents (49%) perceived bribery and corruption as having the most severe impact on their corporate reputation.

From a New Zealand perspective, 4% of those surveyed indicated they had been asked to pay a bribe over the survey period, while 4% also indicated they had lost an opportunity to a competitor which they believe had paid a bribe. While this compares very favourably to a global average of 18%, it is clear to see that New Zealand as a country is not immune from the threats associated with bribery and corruption.

Percentage of respondents asked to pay a bribe



The corporate smuggler

The 'Grey Channel' is a system by which exporters send produce into China, avoiding a range of issues that may otherwise apply, including timing difficulties, health requirements, taxes and export quotas or other limits.

The arrangements appear to be reasonably common practice. The Grey Channel allows goods to reach Hong Kong, with a Chinese or Hong Kong trader taking responsibility for the final export to mainland China, often having re-characterised the nature of the goods (e.g. claiming they were sourced from somewhere other than their actual country of origin).

There seems little doubt that facilitation payments are made to officials in either or both Hong Kong and China, and such payments are most likely illegal.

Despite its apparent common use, the Grey Channel and other similar structures are illegal and the authorities in China and other countries have and will take enforcement action against companies that participate.



Combating bribery and corruption

The Crimes Act 1961 covers offences related to corruption of the Judiciary, Ministers of the Crown, Members of Parliament, law enforcement officers, public officials and the corrupt use of official information. Under the Act, it is an offence to corruptly accept or obtain a bribe for something done (or not done) in an official capacity. Penalties can include terms of imprisonment of up to 14 years.

The Secret Commissions Act 1910 covers bribery and corruption-style offences, which are relevant to the private sector. Penalties can range from a fine of up to \$2,000 or imprisonment of up to two years.

There are also other New Zealand laws which broadly assist the investigation of corruption (the Serious Fraud Office Act 1990) and for the taking of civil sanctions (the Securities Market Act 1978) relating to insider trading and market manipulation.

In addition, New Zealand has also signed the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, as well as the UN Convention against Corruption. Both of these conventions require member countries, such as New Zealand, to implement strong measures to combat bribery and corruption.

Sales and marketing under threat

While the risk of bribery and corruption is a threat to many different types of transactions, it is of particular concern when companies are dealing with government agencies and state-owned businesses – and, consequently, with government officials.

For example: A pharmaceutical organisation would like to sell a recently developed medicine to a country that operates a public healthcare programme. The permission to sell the medicine, the decision to buy it and the price paid will likely be in the hands of government officials.

Or, an equipment company would like to sell their product to a state-owned enterprise whose senior executives are members of the political party currently in office. The specifications in the tender documents, the budget available for the acquisition, the ancillary support services needed for training, spare parts, and maintenance, the evaluation of the bid proposals – all will likely be decided by government officials.

If the territory has a culture that is relatively permissive to bribery and corruption, some of these officials may be predisposed to expect or at least be open to bribes. This exerts pressure on sales and marketing staff, who have been tasked by leadership with bringing a new product to a growing market – pressure which could be felt by individual staff as justifiably offering a bribe or kickbacks, or otherwise rigging the sales process to try and secure a better price.

While the profit potential will likely be obvious to the sales and marketing team, the systemic risk of operating in a culture with a ‘high demand’ component of the corruption equation may be less so. As we have often seen, the US Foreign Corrupt Practices Act (FCPA) and other enforcement tools frequently have far-reaching financial and organisational impacts. These can include altering your sales processes, sales incentives, distribution networks, authority levels and approval requirements for marketing activities and other payments, choice of agents and brokers, and in extreme cases, the ability to operate at all in certain countries.

Competition and anti-trust law

None of our New Zealand respondents reported suffering issues in the competition and anti-trust law sector.

However, the New Zealand Productivity Commission has recently called to have competition law in this country strengthened. The commission argues there are some service sectors that lack intensity of competition which can drive efficiency and productivity gains in the sector. It says the current legislation is flawed and a strengthening of the law is required, specifically in relation to section 36 of the Commerce Act, which deals with the abuse of market power.

Our survey results very much reflect a European focus. The economic profiles of these territories, combined with EU competition laws, appear to be driving a high perception of risk in the region. Of the three economic crimes under the eye of government enforcement mechanisms (bribery and corruption, competition law, and money laundering), competition law was cited as a higher risk by one in four respondents in both Western Europe and Eastern Europe – with Asia Pacific, Africa, and both American continents showing less concern.

It appears that the EU Commission, which has been increasingly aggressive in pursuing high-profile actions against cartel, price-fixing and other forms of market abuse – including in the recent, highly publicised LIBOR affair – is having a definitive impact on the concerns and operations of EU-based companies.



High impact economic crimes

Procurement fraud: A growing opportunity, a growing threat

Procurement fraud, defined for the purposes of our survey as ‘illegal conduct by which the offender gains an advantage, avoids an obligation or causes damage to his organisation. The offender might be an employee, owner, statutory board member, an official, a public figure or a vendor who was involved in the purchase of services, goods or assets for the affected organisation’ – was added as a distinct category to this year’s survey.

Generally, when an organisation goes into a commercial or public tender process or seeks to acquire goods and services for its own use – a common process across all industries – the potential for procurement fraud exists.

19%

of New Zealand respondents who experienced economic crime reported occurrences of procurement fraud.

2nd

most reported fraud – after asset misappropriation.

28%

of New Zealand respondents believe they are likely to encounter procurement fraud over the next 24 months.

We anticipate that the significant response in this category is driven by the fact that New Zealand is in a period of growth due to the property rebuild in Canterbury and the significant housing construction activity in Auckland.

In addition, there has been an increase in more competitive public tender processes from governments and state-owned businesses, unleashing the possibility of fraudulent activity on the part of agents and other third parties. No doubt, in past surveys, procurement-related kickbacks, bid-rigging, or similar activities were reported as corruption. But with our new inquiry into where in the process procurement fraud primarily occurred, the connection has become clearer. Of the New Zealand respondents, 40% said procurement fraud had occurred during vendor selection, in the payment process and during vendor contracting / maintenance.

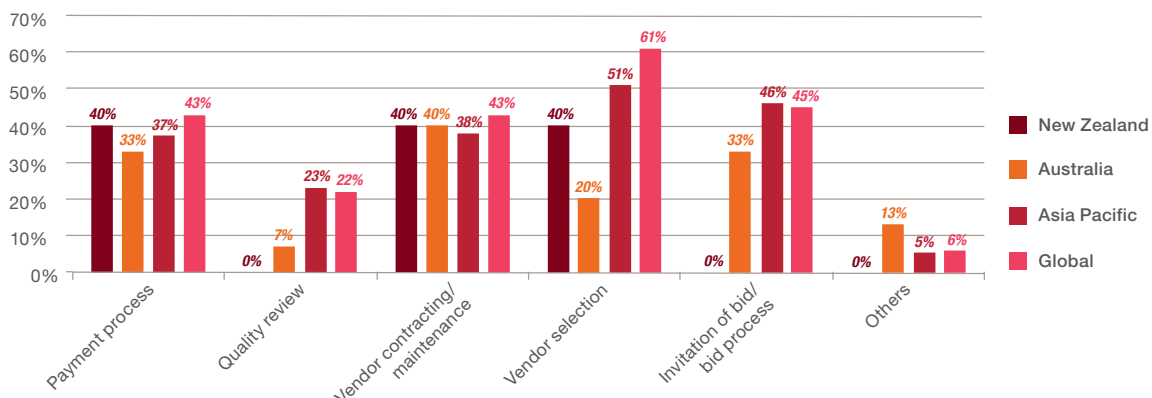
Moreover, our recently launched 2014 Global CEO Survey highlights a significant majority of businesses are focusing on

making changes to their supply chain in response to global trends. Many are seeking deeper interconnections across their value chain, and using a more global supply model. And as suppliers become more integrated into companies’ operations, the threat of significant disruption and monetary loss increases.

In addition, as economies have emerged from the recent economic crisis, a shift in employment practices seems to have occurred. Short-term, post-crisis measures, such as replacing permanent, in-house positions with more dispensable and scalable outside resources, have persisted with companies more willing to outsource tasks once part of their non-core and core operations.

Based on these responses, we see procurement fraud as a double threat. It victimises businesses in their own acquisition of goods and services. And it prevents companies from competing fairly and successfully for business opportunities subject to a commercial or public tender process.

Procurement fraud occurrence by stage



Procurement fraud by industry

In New Zealand, the industries that reported the most procurement fraud were core government and state owned industries (43%), engineering and construction (4%) and transport and logistics (4%). These sectors are heavily reliant on large outside suppliers and therefore the likelihood of procurement fraud is heightened.

Threats to the purchasing process

While our discussion has focused on external parties, it is important not to overlook the threat from within. In our experience, the requisitioning of goods is an area ripe for fraud. The threat is especially great in cultures where loyalty to family, friends, local community, or even national pride are strong influences – stronger perhaps than dry corporate policy statements or legalistic-sounding codes of conduct.

An individual within the purchasing and supply department may have a pre-existing relationship with a vendor who wants to win business from the organisation. The insider provides information on the bidding process, such as the bid amounts of competitors, to ensure an advantage for their preferred bidder. Or, the insider could approve a price higher than necessary.

Alternately, your controls may not function as planned. We have observed countless incidences of employees in approval roles acquiescing to pressure from ‘the boss’ to process payments that do not meet all aspects of policy and procedure. This tension between an executive’s loyalty to the company versus their connectivity to the local milieu is a real and continuing threat to controls.

In our experience, the requisitioning of goods is an area ripe for fraud.



Asset misappropriation

Asset misappropriation, more commonly known as theft, is by far the most common economic crime experienced by organisations reporting fraud, with 70% of respondents suffering from it. This amount is more than three times the second highest occurring type of economic crime, procurement fraud (19%). While the individual impact of this fraud may be lower than that of cybercrime or government-enforced frauds, subject to specific enforcement regimes, the magnitude of the threat requires organisations to be vigilant.

(Not) falling off the back of a truck

This euphemism for asset misappropriation points to one of the fundamental business processes it attacks – distribution, logistics and warehousing.

For example, take a global operating retail company with warehouses of inventory. Not only are these products exposed to the organisation's own employees, they also constantly pass through the hands of third parties, leading to several points of vulnerability in the supply chain and distribution process. Schemes can be as simple as employees stealing inventory or more complicated endeavours, such as covering up a theft by marking good inventory as 'scrap', removing it from the premises, and then reselling it.

Another function which is commonly threatened by asset misappropriation is the expense reporting process – which further impacts on the cash disbursement function and potentially leading to collateral impacts, such as inaccurate books and records. Further, disbursements to employees which are illegitimate affect cash on hand and increase expenses.

Are you protecting what matters most?

Intellectual property (IP) infringement and theft is often an especially damaging economic crime – and one that is very much on the mind of New Zealand CEOs, 31% of whom reported they are worried about being able to protect it, according to our Annual Global CEO Survey.

In our cybercrime section, we noted that organisations should focus their cyber security on protecting these crown jewels, rather than on just their network. In certain industries, intellectual property is the key asset that allows the company to win in the marketplace. Thirteen percent of New Zealand respondents indicated they expect to be threatened by this economic crime in the next 24 months, compared with none who actually reported occurrences in the survey period.

The gap between expectations and experience is a consistent theme in the area, and we believe it demonstrates another concept: successful crimes which target assets often go undetected or unreported. Our respondents appear to be aware that their IP is at risk, but their controls may not be detecting the actual attacks.

Accounting fraud: The connected threat

Accounting fraud has always been one of the major crimes reported in our survey, and since 2005, has been cited by over 20% of our global respondents that experienced economic crime. This year was no exception with a global response rate of 22%. The picture is somewhat different in New Zealand, as only 7% of New Zealand respondents who had suffered economic crime report occurrences of accounting fraud.

Cybercrime: The risks of a networked world

The advancement of technology in business services, combined with the explosive growth in social media and data connectivity, has permanently altered, and in many ways, brought together the business and consumer landscapes.

Unfortunately, connectivity and access also have a dark side – one which empowers motivated, sophisticated criminals who are able to operate below the radar. And because cybercrime operates largely unseen, organisations may never realise they are being targeted until long after the damage is done.

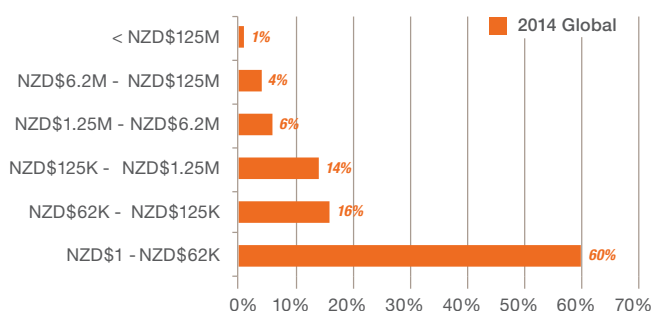
This fact alone makes the many varieties of electronic fraud one of the most threatening types of economic crime.

Our 2011 Global Economic Crime Survey was the first in our series to highlight cybercrime as a high-level threat to organisations. This year's survey confirms the significant, continuing impact of this crime on business, with now one in four global respondents reporting they have experienced a cybercrime – and over 11% of these suffering financial losses of more than US\$1 million.

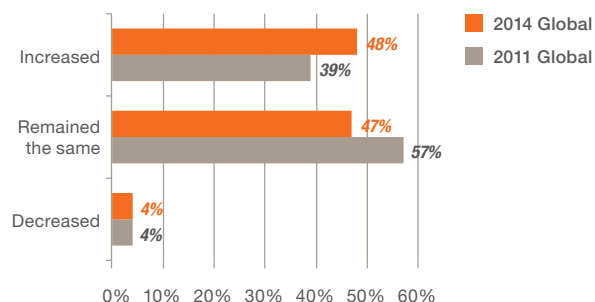
In a sign that organisations are taking this threat more seriously, our survey indicates that the perception of the risk of cybercrime is increasing at a faster pace than that of reported actual occurrences. This year, 48% of our global respondents said their perception of cybercrime risk at their organisation increased, up from 39% in 2011.

Reinforcing this, 40% of New Zealand CEOs in our latest Annual Global CEO Survey said they were concerned about cyber threats, including the lack of data security.

Relative impact of cybercrime on organisations



Perception of cybercrime



40% of New Zealand CEOs in our latest Annual Global CEO Survey said they were concerned about cyber-threats, including the lack of data security.

What you don't know can hurt you

While one quarter of respondents reporting they have suffered a cybercrime is concerning enough, we must also consider that a significant percentage of those who did not report cybercrime may also have suffered an event – and not even know about it.

This underscores the challenge of the threat. Many entities do not have clear insight into whether their networks and the data contained therein have been breached, and they don't know what has been lost – or its value.

Further complicating the picture is a third aspect of the lack of transparency into cybercrime events: even when it is detected, cybercrime often goes unreported. Outside of privacy breaches in regulated areas such as 'identity theft', there are few regulatory conventions requiring disclosure. And often – such as in the case of theft of key intellectual property – there may be compelling competitive reasons for organisations to keep such losses confidential.

For example, if a confidential bid planning document were accessed by cyber criminals and utilised by rivals to gain an advantage, would a company disclose the incident? Are organisations adequately defending against such cybercrime breaches, and if they were discovered, how would they value the loss?

The bottom line is that much of the damage caused by these kinds of attacks is not disclosed, either because it is not known, because it is difficult to quantify, or because it is not shared.

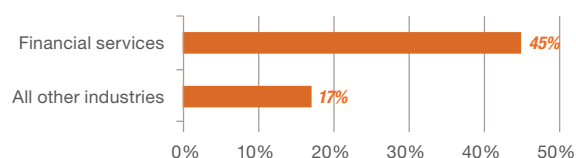
Focus on financial services

Forty-five percent of global financial services organisations affected by fraud reported being victims of cybercrime – nearly twice the frequency as reported by all other industry sectors.

Why such a large percentage? Large, regulated financial institutions often have more and better system safeguards – which may increase the chance of a breach being detected. In addition, banks are where the money is.

Finally, financial institutions are an appealing target because they provide large amounts of customer and personal financial information online, which can potentially be accessed – and sold on the black market – as a precursor to organising a theft of funds.

Cybercrime impacting financial services



A moving target

In a changing technological landscape, the sophisticated adversary takes advantage by attacking new weaknesses. This is why it is essential for organisations to at least try to keep pace with the criminals who threaten them.

Even when organisations are generally aware of the types of cyber threats they face, many do not truly understand the capabilities of cyber criminals, what they might target, and what the value of those targets might be. Yet, companies continue to make their critical data available to management, employees, vendors, and clients on a multitude of platforms – including high-risk platforms such as mobile devices and the cloud – because the economic and competitive benefits appear so compelling.

The uptake of ‘cloud services’ is also driving behavioural change, both at business and consumer levels. The ‘digital disruption’ of what were bricks and mortar businesses are forcing organisations to move quickly to embrace new sales channels, leveraging cloud services to do so. This introduces a more complex technology and business relationship which is proving to be a fertile ground for potential cyber criminals to exploit.

‘Spear phishing’ attacks, historically focused on financial institutions, are now being seen targeting retail consumers via social media. This connectivity, and simple fact that humans will normally use the same credentials for multiple systems, means a simple compromise of one set of access credentials could easily unlock a person’s complete identity. A recent extension of this is the latest ransomware outbreaks, where a user’s complete computer is encrypted

and a ransom has to be paid to release the decryption key. While in the true sense this is not a new phenomenon – the scale, complexity and sheer brashness of these attacks on the public are unprecedented.

While nobody expects the benefits of technology to diminish, or for organisations to shrink their digital footprint, it’s clear that – with more data accessible on more platforms – valuable data will remain under attack, and the cost of security breaches will continue to be steep. In fact, in every region, between a quarter and a third of organisations told us they believe they will likely encounter cybercrime in the near future.



Cybercrime is a strategic problem

Ultimately, cybercrime is not just a technology problem. It is a strategy problem, a human problem and a process problem.

After all, organisations are not being attacked by computers, but by people attempting to exploit human frailty, as much as technical vulnerability. As such, this is a problem which requires a response that is grounded in strategy and judgement about business process, access, authority, delegation, supervision and awareness – not merely tools and technologies.

This is illustrated in at least four ways. First, knowing that people are often the weakest link in the security chain, hackers often exploit human naiveté through attacks such as ‘spear phishing’ – a targeted email approach supposedly sent from a source that you trust, such as your bank – to take advantage of the inattentive. Alternatively, hackers can try to break data encryption codes through the brute computing power of modern machines, or they can guess at, steal, or bribe their way to possession of an easy password.

Second, hackers ‘productivity’ improves not only through the use of new technology, but also through the better-organised use of people in the ‘mule’ capacity.

Third, cyber security solutions often require non-technical processes and tools – for example, training and awareness, and the involvement of legal and privacy experts for response, media relations, crisis management and remediation solutions in the wake of uncovering a cybercrime.

Finally, good security requires people to remain focused on their most important data. Companies that prioritise the data on their networks are able to focus on the ‘crown jewels’ – and spend their limited cyber security budgets wisely.

Thus, one of the key organising principles of cyber security is not a technical question for the IT staff at all. It is a business question for senior managers. Yes, your IT team has to know what the best tools and technologies are for your business, but know that will do little good if you are focused on protecting the wrong assets.



Cybercrime threatens technology-enabled business processes

The growing use of technology-enabled business processes makes cybercrime a very real threat to a wide variety of business operations. In our recent experience, the systems most threatened are those that contain data directly leading to financial assets that can be stolen or personal data that can be used to assemble an attack on financial assets. Technology-enabled business processes that are threatened by cybercrime include:

- **Point of sale purchases** by debit and credit cards in the everyday retail environment.
- **ATM transactions** in the everyday banking environment.
- Preserving or respecting the **privacy of customers**. This is especially true in the health care industry where providers often maintain systems with considerable amounts of sensitive patient information, including identity, financial circumstances, insurance plans, and medical conditions.
- **E-commerce or on-line sales processes**. Same issues as penetration of point of sales systems in the retail store or banking environment, except that it is in the on-line environment.
- **Electronic business communications (email)**. External cyber criminals can penetrate corporate communications systems and steal critical commercial information, intellectual property, and sensitive executive communications.
- Taking advantage of **infrastructure weak points** to accomplish any of the above – for example, penetrating Wi-Fi access points or intercepting other people’s communications through them; attacking business operating systems using ‘cloud’ architecture by penetrating the server environment maintained by the cloud provider.
- **Consumer incentives**. Loyalty and other consumer incentive programmes that retain customer data and spending habits/preferences offer a treasure trove of data that can be used for identity theft and targeting for additional cybercrime.
- **M&A**. After the completion of a merger or acquisition, the company will often delay full integration of information security policies, processes and tools. This leaves vulnerabilities in a corporate IT environment which hackers can exploit – for example, by gaining access to databases from legacy enterprises that contain valuable intellectual property or other types of sensitive data.
- **Supply chain**. Suppliers, contractors and distributors are part of a company’s ecosystem – often with authorised staff-like access to sensitive data and systems. Their risk is your risk, and a breach in the supply chain can have cascading effects on network security, or worse, allow direct access to sensitive data.
- **Research, development and engineering**. Proprietary technology, trade secrets, and intellectual property are targeted by nation-states, state-owned enterprises, and unethical corporations. Businesses have lost billions of US dollars in this way through theft by hackers and insiders of intellectual property to the benefit of competing organisations.
- **Expansion into new markets**. As a company moves into a new geographical market, it can become the target of the host government or local competitors who want to steal its technology, client lists or marketing plans. As the company is literally on another’s ‘home turf’, the insider problem extends beyond employees, to facility providers, talent search firms, janitorial services, even local government agencies.



Identifying the fraudster

Know your enemy

Trying to profile a typical fraudster is difficult, but gathering as much information as possible on these individuals is important. Profiling can help to identify weaknesses in existing control environments, and as a result, allows for more targeted controls to be identified and implemented.

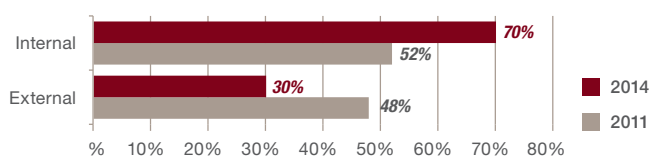
We asked respondents whose organisations had experienced economic crime, to profile the main perpetrators of the most serious frauds they had suffered. The results were interesting and very different to previous years. In 2014, 70% of New Zealand respondents reported that the main perpetrator of fraud was an internal party, whereas 30% reported the main perpetrator as being an external party. In 2011, the results were evenly split.

However, the one thing that remains constant among New Zealand respondents is the fact organisations in the financial services and retail sectors suffer far more fraud attacks from outside their organisations. This trend is potentially linked to the disproportionately high rate of cybercrime affecting financial services and the fact that cybercrime tends to involve perpetrators from outside an organisation.

On the other hand, New Zealand respondents in transport and logistics, as well as the government sector, reported all their occurrences of fraud came from internal perpetrators.

The silver lining of having most of one's fraud losses attributable to internal players – people you have some visibility over – is that there is good potential to mitigate the risks through improved internal policies, processes and controls. As we will see, this is more challenging with external fraudsters.

Internal vs external fraudsters



What increases the likelihood of fraud?

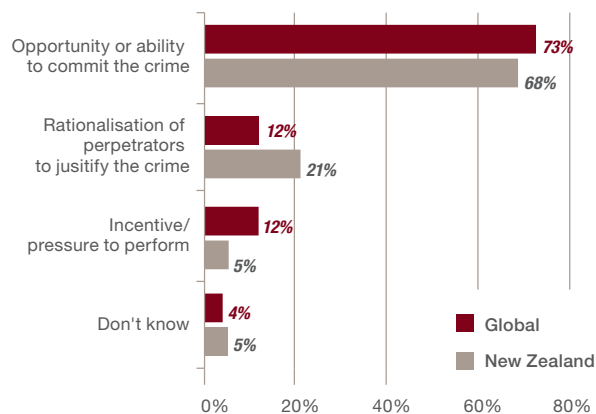
Anti-fraud practitioners commonly refer to a ‘fraud triangle’ – the three elements that are often present when a perpetrator commits fraud: pressure, opportunity and rationalisation.



This year we asked respondents what factor they felt had contributed the most to economic crime committed by internal parties. Almost 70% of New Zealand respondents indicated that the opportunity or ability to commit the crime was the factor that most contributed to economic crime, which is broadly in line with the global average of 73%.

While this news may at first seem anti-climactic, it's important to keep in mind that, of the three factors, opportunity is the one most in an organisation's control. The implication is that while life's pressures and the ability to rationalise may swirl around employees, if an organisation can limit the opportunity, they can do much to stop the fraud before it starts.

Why does fraud occur in New Zealand?



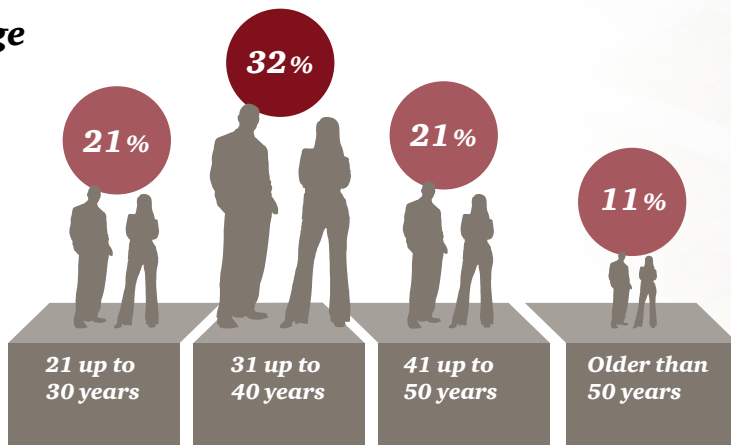
While we cannot plot the specific pressure or rationalisation behind each internal act of fraud, we can at least profile the fraudster. We asked respondents who had pointed to an internal party as the main perpetrator of economic crime to profile the fraudsters age, gender, length of service, and education level.

Our results indicate that the overall profile of the internal fraudster in New Zealand generally remained the same as in 2011 – middle-aged males, educated only to high school level or less, who have been with the organisation for five years or less.

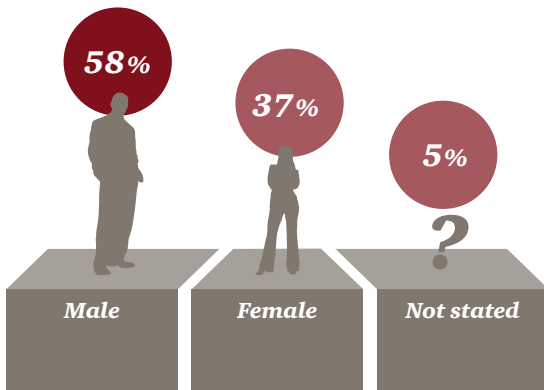
Globally, we did note some differences in certain regions and industries. For example, the percentage of senior management committing internal fraud in the Middle East was 25% higher than the global average, while in Latin America the percentage of junior staff committing internal fraud was 13% higher than the global average.

New Zealand's typical internal fraudster

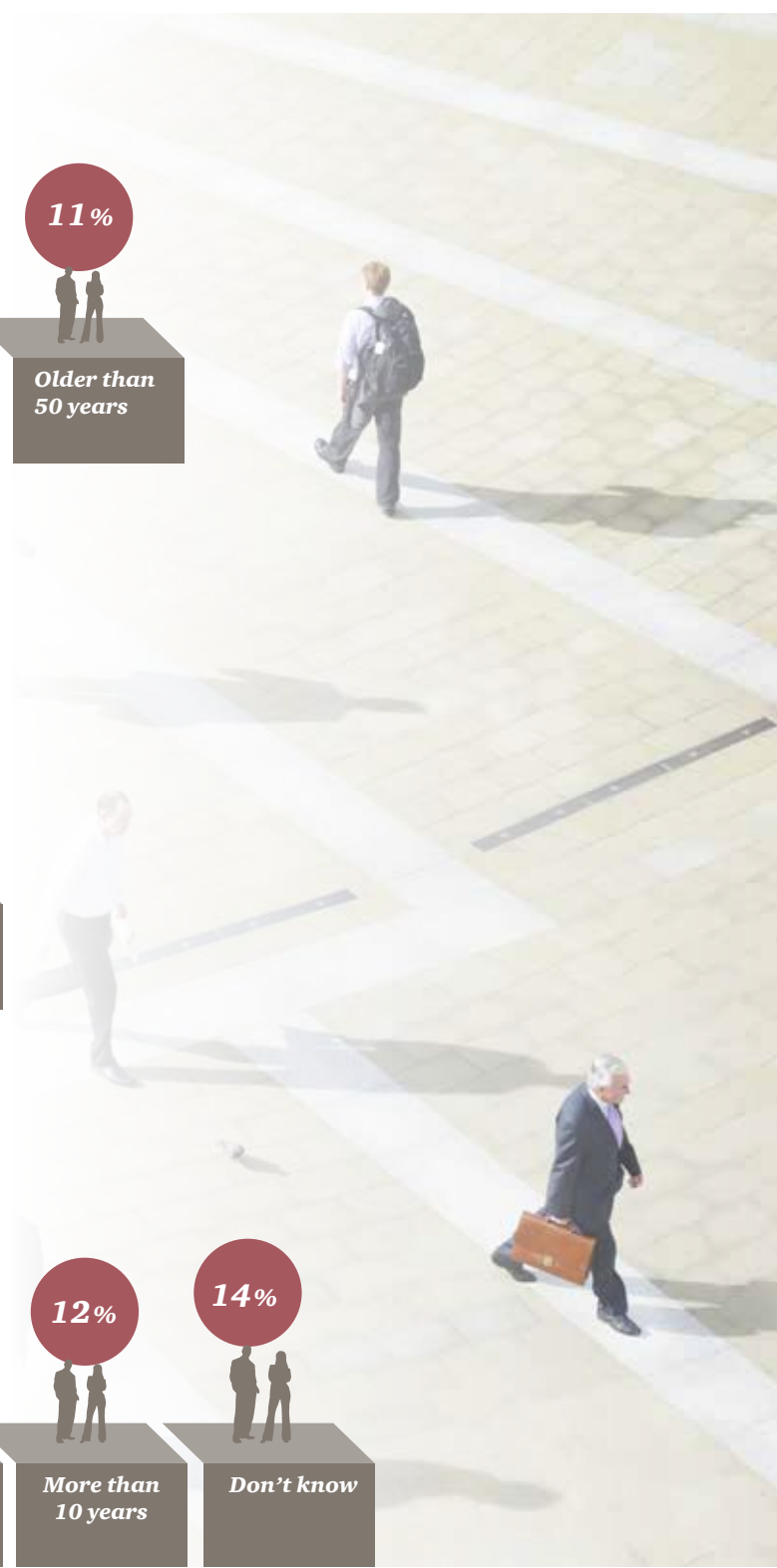
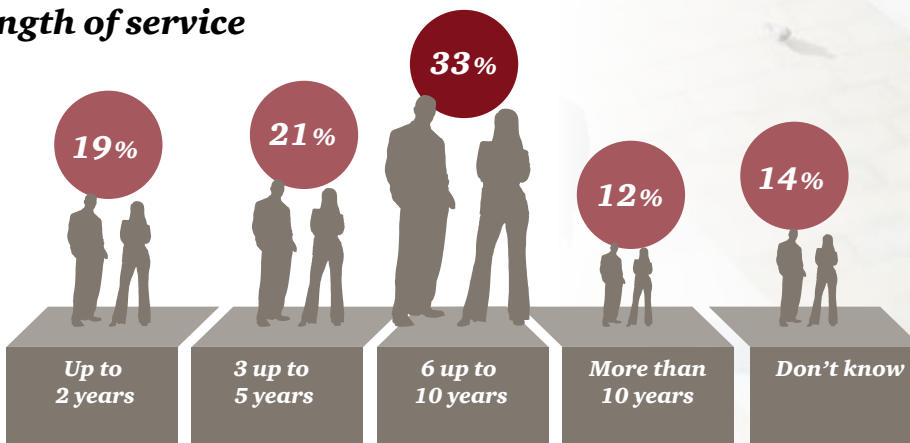
Age



Gender



Length of service

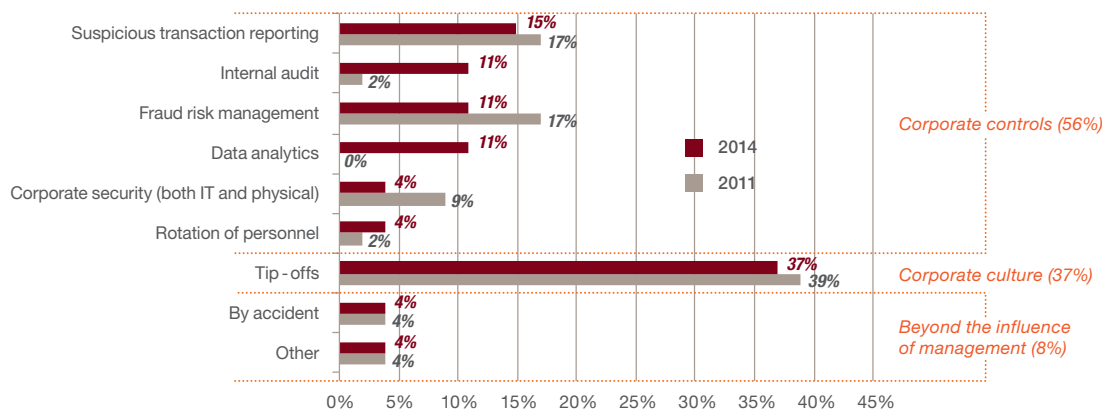


To catch a thief

Fraud is detected by various corporate controls, tip-offs and events beyond the influence of management.

The below graph shows the methods by which major fraud was detected by organisations across New Zealand, over the last 24 months.

Detection methods



Note: Data analytics was only added as a category in 2014.

The graph highlights the significance of a tip-off and avenues for tip-offs as the most effective method of fraud detection.

Our results indicate that 71% of New Zealand respondents now have a whistleblower mechanism in their organisation, with 22% of these respondents rating the service as effective, while a further 5% rated it as very effective.

Tip-offs, both external and internal, including via a formal whistleblowing channel, accounted for 37% of all methods by which frauds were discovered. This is consistent with the results from previous years and similar to other studies¹. This is good news for New Zealand, as it appears that organisations here are realising the value of whistleblower hotlines as an effective forum for people to report concerns.

On 30 June 2013, the AML/CFT Act came into force. Compliance with this Act has meant that affiliated businesses operating in New Zealand have invested significant time and resources to ensure they have effective controls in place to monitor customer accounts and associated transactions. Many of these controls have been implemented through the use of electronic systems, which is likely linked to the high percentage of fraud detected through suspicious transaction reporting and data analytics.

Internal audit is now responsible for 11% of frauds discovered. This is back to pre Global Financial Crisis levels, having dropped significantly previously (2011: 2%). This may indicate that companies here are also beginning to refocus their efforts and investments when it comes to resourcing internal controls and internal audits teams.

¹ ACFE 2012 Global Fraud Study, Initial Detection of Occupational Frauds from 'Tip', 43.3% and in 2010, 40.2%

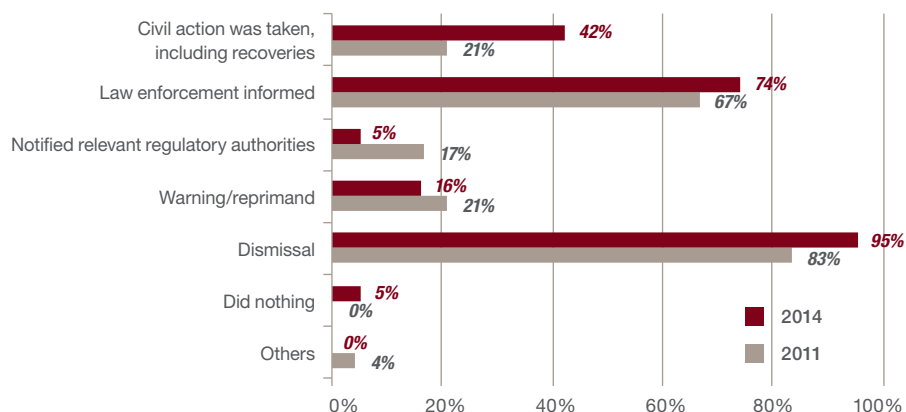
Actions taken against fraudsters

This year's survey confirms that organisations continue to respond to internal fraud aggressively, with 95% saying they are dismissing perpetrators once detected. Overall, the results indicate that aggressive actions such as dismissal (95%), informing law enforcement (74%) and civil action (42%) are on the increase.

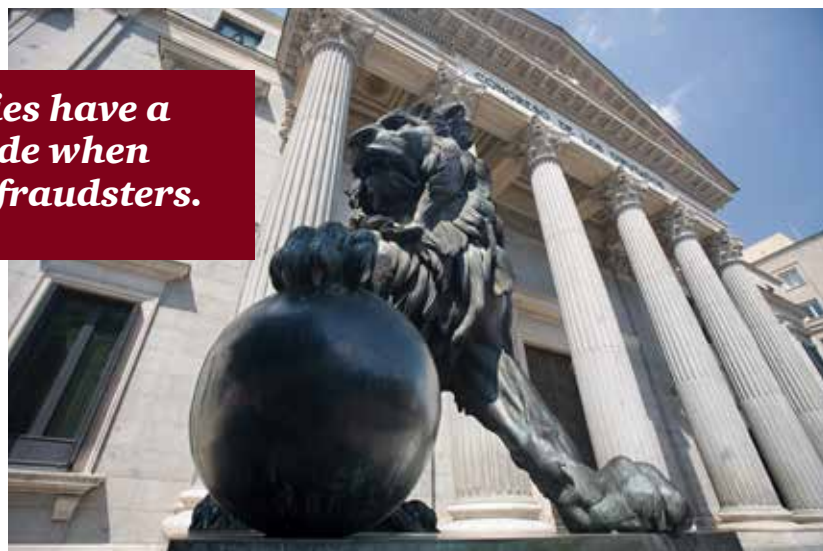
This indicates that New Zealand companies have a 'zero tolerance' attitude when dealing with internal fraudsters, with organisations now more willing to deal with fraudsters through official channels. The 12% increase in dismissals suggests that organisations see these fraudulent employees as detrimental to their organisations and are not afraid to replace them.

Civil action, including recoveries, has doubled since 2011, which suggests that response procedures are becoming more mature and effective, with organisations now more devoted to not just dismissing the fraudster but recovering their losses too.

Actions taken against internal fraudsters in New Zealand



New Zealand companies have a 'zero tolerance' attitude when dealing with internal fraudsters.



The external fraudster

There has been a substantial change in the overall profile of the external fraudster since 2011. The number of frauds carried out by vendors and agents/intermediaries has significantly increased with the former now accounting for 25% of external fraud occurrences (2011: 9%) and the latter also accounting for another 25% (2011: 14%).

This increase is potentially linked to the large number of respondents (49%) we had in the following industries:

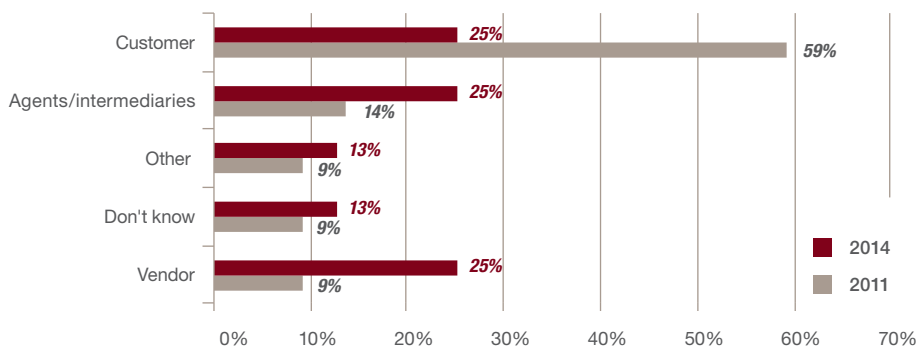
- Energy, utilities and mining (9%)
- Engineering and construction (6%)
- Government/state-owned enterprises (22%)
- Transportation and logistics (10%)

These industries are particularly vulnerable to external fraud from vendors and intermediaries, primarily because they have outsourced many

non-core (and in some cases core) elements of their value chains, with a resulting increase on reliance on suppliers and intermediaries.

We also noted that the number of frauds carried out by customers was significantly down (25%) (2011: 59%), while worryingly, there was a significant increase in respondents who reported a 'don't know' when asked to profile the fraudster. As mentioned previously, knowing your enemy is imperative when combating economic crime, especially if trying to recover costs and identify better controls.

Profile of the external fraudster



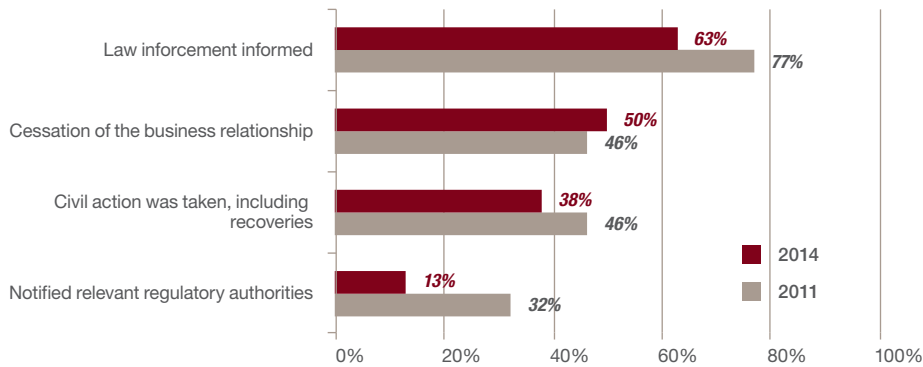
Knowing your enemy is imperative when combating economic crime, especially if trying to recover costs and identify better controls.

Confront an external fraudster

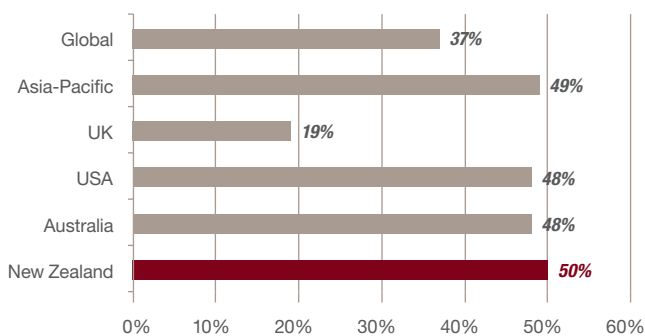
Consistent with previous years, the most common action taken against an external perpetrator in New Zealand was informing law enforcement (63%). The global average was 61%.

In addition, New Zealand companies appear to have little tolerance when it comes to dealing with third-party related fraud, with 50% of our respondents ceasing business relationships. This is similar to other developed economies, such as Australia (48%) and the USA (48%), and regionally puts us on a par with the Asia-Pacific average (49%).

Actions taken against external fraudsters



Cessation of business relationships



Who did we survey?

48

questions to assess corporate attitudes, approaches and experience to fraud in the current economic environment

22%

of organisations operate in government and state-owned enterprise sectors

82

New Zealand respondents

37%

of all respondent companies had between 501 – 1,000 employees

43%

of all respondents were CFOs

74%

of those who had suffered some form of economic crime reported less than 10 incidents over the past 24 months

63%

of companies surveyed operate in New Zealand only

63%

of respondents estimated that the financial loss associated with incidents of economic crime was less than NZ\$60,000

Appendix

Purpose of the 2014 survey

The aim of our survey was to assess corporate attitudes, approaches and experiences to fraud 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 bribery/corruption, money laundering and anti-competition, and what types of fraud are most common.

Terminology

Accounting fraud

Financial statements and/or other documents are altered or presented in such a way that they do not reflect the true value or financial activities of the organisation. This can involve accounting manipulations, fraudulent borrowings/raising of finance, fraudulent application for credit and unauthorised transactions/rogue trading.

Asset misappropriation, including embezzlement/deception by employees.

The theft of assets (including monetary assets/cash or supplies and equipment) by directors, others in fiduciary positions or an employee for their own benefit.

Bribery and corruption

The unlawful use of an official position to gain an advantage in contravention of duty. This can involve the promise of an economic benefit or other favour, the use of intimidation or blackmail. It can also refer to the acceptance of such inducements. Specific examples include kickbacks, extortion, gifts (with strings attached), facilitation payments, etc.

Competition law/anti-trust law

Law that promotes or maintains market competition by regulating anti-competitive and unfair business practices conduct by organisations. Examples may include price fixing, excessive, predatory or discriminatory pricing, unfair trading terms, and tying (i.e. stipulating that a buyer wishing to purchase one product must also purchase all or some of his requirements for a second product).

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, illegal downloads of media, phishing and pharming and theft of personal information such as bank account details. This excludes routine fraud whereby a computer has been used as a byproduct 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.

Economic crime

The intentional use of deceit to deprive another of money, property or a legal right.

Espionage

Espionage is the act or practice of spying or of using spies to obtain secret information.

Financial loss

When estimating financial losses due to fraud, the participants should include both direct and indirect loss. The direct losses are the actual amount of fraud and the indirect losses would typically include the costs involved with investigation and remediation of the problem, penalties levied by the regulatory authorities, and litigation costs. This should exclude any amount estimated due to 'loss of business opportunity'.

Financial terms

When estimating financial losses due to fraud, the participants should include both direct and indirect loss. The direct losses are the actual amount of fraud and the indirect losses would typically include the costs involved with investigation and remediation of the problem, penalties levied by the regulatory authorities, and litigation costs. This should exclude any amount estimated due to 'loss of business opportunity'.

Fraud risk assessment

Fraud risk assessments are used to ascertain whether an organisation has undertaken an exercise to specifically consider:

- i. The fraud risks to which operations are exposed;
- ii. An assessment of the most threatening risks (i.e. Evaluate risks for significance and likelihood of occurrence);
- iii. Identification and evaluation of the controls (if any) that are in place to mitigate the key risks;
- iv. Assessment of the general anti-fraud programmes and controls in an organisation; and
- v. Actions to remedy any gaps in the controls.

Human resources fraud (recruitment and/or payroll fraud)

Fraud committed by members of the human resources department, including payroll fraud, ghost employees, pay-to-work, recruitment (i.e. hiring friends and/or relatives, hiring unqualified individuals, falsification of documents, etc.).

Incentive/pressure to perform

The individual has some financial problem that he/she is unable to solve through legitimate means so he/she begins to consider committing an illegal act as a way to solve the problem. The financial problem can be professional (e.g. job is in jeopardy) or personal (e.g. personal debt).

Insider trading

Insider trading refers generally to buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, non-public information about the security. Insider trading violations may also include 'tipping' such information, securities trading by the person 'tipped', and securities trading by those who misappropriate such information.

IP infringement (including trademarks, patents, counterfeit products and services)

This includes the illegal copying and/or distribution of fake goods in breach of patent or copyright, and the creation of false currency notes and coins with the intention of passing with off as genuine.

Markets with a high level of corruption risk

While corruption risk levels can be subjective, for the purposes of this survey we suggest a territory with a Transparency International Corruption Perception Index (CPI) score of 50 or less be considered a market with a high level of corruption risk. The link below the responses will direct you to the Transparency International list of territories and CPI scores.

Money laundering

Actions intended to legitimise the proceeds of crime by disguising their true origin.

Mortgage fraud

Mortgage fraud schemes employ some type of material misstatement, misrepresentation, or omission relating to a real estate transaction which is relied on by one or more parties to the transaction.

Opportunity or ability

The individual finds some way that he/she can use (abuse) his/her position of trust to solve the financial problem with a low perceived risk of getting caught.

Procurement fraud

Illegal conduct by which the offender gains an advantage, avoids an obligation or causes damage to his organisation. The offender might be an employee, owner, statutory board member, an official, a public figure or a vendor who was involved in the purchase of services, goods or assets for the affected organisation.

Rationalisation

The individual finds a way to justify the crime to himself/herself in a way that makes it an acceptable or justifiable act.

Tax fraud

An illegal practice where an organisation or corporation intentionally avoids paying its true tax liability.

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 measures to better protect themselves from fraud.

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