Exploring the big cyber questions

A New Zealand context

Global State of Information Security Survey 2016

65%

of NZ respondents have confidence that their information security activities are effective.

41%

of NZ respondents have accurate inventory of personal data for employees and customers.

35%

of NZ respondents classify the business value of data.

pwc

www.pwc.co.nz/gsiss2016

Contents

Foreword

Welcome to our New Zealand insights for the PwC Global State of Information Security Survey.

I'd like to express my sincere thanks to the Government, business and information technology leaders who took the time to participate. This is PwC's 18th year conducting this survey, which provides a forum for private and public sector organisations around the world to voice their views on the state of information security today and where we'll be tomorrow.

This survey of worldwide information security practices is conducted annually by PwC, in partnership with the publisher of CIO Magazine, to understand how executives and industry leaders view current and future challenges related to cyber security. In essence, it shines the spotlight on what organisations are doing – and plan to do – when it comes to managing the real business risk associated with their information systems and data.

For most organisations, their information systems and data have become critical assets when it comes to performing core functions and maintaining the trust of their stakeholders. So given the dynamic and ever-evolving risk landscapes in which they operate, it's important to focus on the assets that matter the most.

We live in a world of mobile payments, cloud services, a mobile workforce and a growing interdependence on other organisations. In fact, in our annual New Zealand CEO Survey, 84 per cent of chief executives told us that mobile technologies were important for their digital strategies and 50 per cent told us they are looking at entering into a joint venture or strategic alliance this year.

This means that the outdated approach of treating this as a technical issue and focusing on protecting an organisation's digital perimeter has limited relevance in today's interconnected world. Each day, whether or not they realise it, New Zealand organisations are suffering financial losses, operational disruption and reputational damage because of security incidents.

The organisations that want to maintain trust and stay competitive are those using a targeted information security approach. Far too often we see organisations investing and managing their risk poorly by implementing elements of security strategies simply because they see others doing it. To have an effective strategy, organisations must invest the time to understand which assets are most important to them, and then focus resources on dynamically protecting them by being in a position to detect, respond and recover when there is an incident.

When you understand what is important to you, it becomes much easier to appreciate the big business questions this survey challenges us to address. We hope that the insights in these pages will help you on your journey to answer these game-changing questions for your organisation.

Adrian van Hest
Partner and Cyber Practice Leader

The global context
A new normal

31.3%

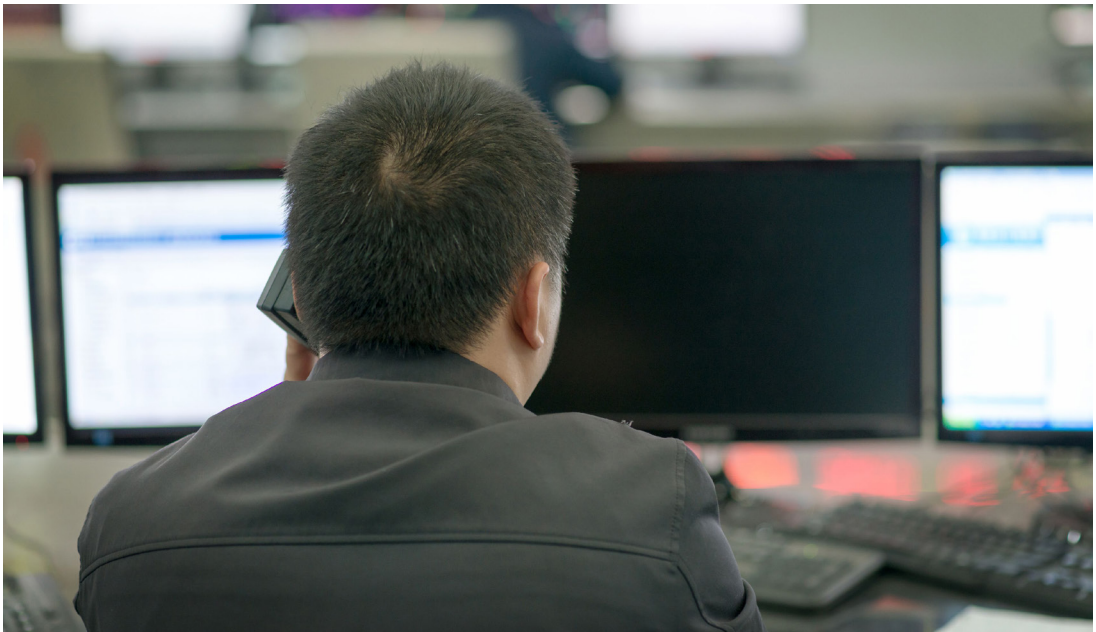
of NZ respondents do not have an overall security strategy but plan to make it a priority in the coming year.

Worldwide, cyber attacks have become the new normal in today's digitally connected world. Existing information security methods have proved ineffective, which is why many organisations are rethinking their cyber security strategies and practices.

Historically in New Zealand, organisations have assumed this is a technology issue and been focused on preventing incidents by spending money on technology such as firewalls, simple access management and anti-virus software. This approach assumes that all you need to do is to stop threats at the perimeter of an organisation.

Many businesses are charting an entirely new course when it comes to technology to take advantage of emerging platforms and opportunities, leaving the concept of a digital perimeter far behind. These include the internet of things, mobile payment systems, cloud computing, the use of DevOps and open-source software. This dynamic shift requires a new approach to security.

In terms of security strategies for mobile devices, 50.5 per cent of New Zealand organisations say they have a strategy in place, compared to 47.6 per cent globally. Despite being an early adopter of technology (such as smart meters with one of the largest numbers of mobile to mobile or embedded mobile cellular subscriptions per inhabitants in the Organisation for Economic Co-operation and Development) it's a different story for the internet of things. In New Zealand, 24.5 per cent of organisations have no plans to implement a security strategy for the internet of things, compared to just 9.9 per cent globally who have no plans for such strategy.



While many New Zealand organisations have indicated a security strategy for individual technologies and processes, 31.3 per cent of respondents do not have an overall security strategy but plan to make it a priority in the coming year.

In addition to new technologies and processes, many organisations are emphasising the people side of the cyber security equation. Take, for example, expanding the roles of top security executives, CEOs and the boardroom.

The survey data suggests that New Zealand is slightly behind the curve in the boardroom. Globally, 34.8 per cent of organisations say a chief information security executive delivers risk updates at least four times a year to the board. In New Zealand, only 20.6 per cent receive regular updates.

Globally, organisations have boosted information security spending by 24 per cent over last year and are gearing up to tackle the cyber security juggernaut head on.

24.5%

of NZ respondents have no plans to implement a security strategy for the internet of things.

What are the common risk-based cyber security frameworks globally?

NIST Cybersecurity Framework: The US Commerce Department's National Institute of Standards and Technology (NIST) framework provides a structure that organisations, regulators and customers can use to create, guide, assess or improve comprehensive cyber security programmes.

ISO 27001: This is an information security standard published by the International Organization for Standardization (ISO). It is a specification for an information security management system (ISMS). Organisations which meet the standard may gain an official certification issued by an independent and accredited certification body on successful completion of a formal audit process.

Information Security Forum Standard of Good Practice: Updated annually, this is the most comprehensive information security standard in the world and provides more topic coverage than ISO. This standard enables compliance with ISO and other internationally known standards.

SANS Critical Controls: Published by the SANS Institute, this guide does not attempt replace NIST, but instead prioritise and focus on a smaller number of actionable controls with high payoff. In short, these guidelines aim for a must-do-first philosophy.

Advances in computer science and technologies are providing a transformational opportunity for organisations to revise their cyber security strategies. Indeed, companies that embrace new approaches to cyber security can rethink legacy technologies and processes, as well as achieve competitive advantages through operational and cost efficiencies. Organisations are implementing technologies – such as cloud-enabled security, data analytics and advanced authentication – as well as processes, such as risk-based frameworks, external collaboration and the purchase of cyber insurance.

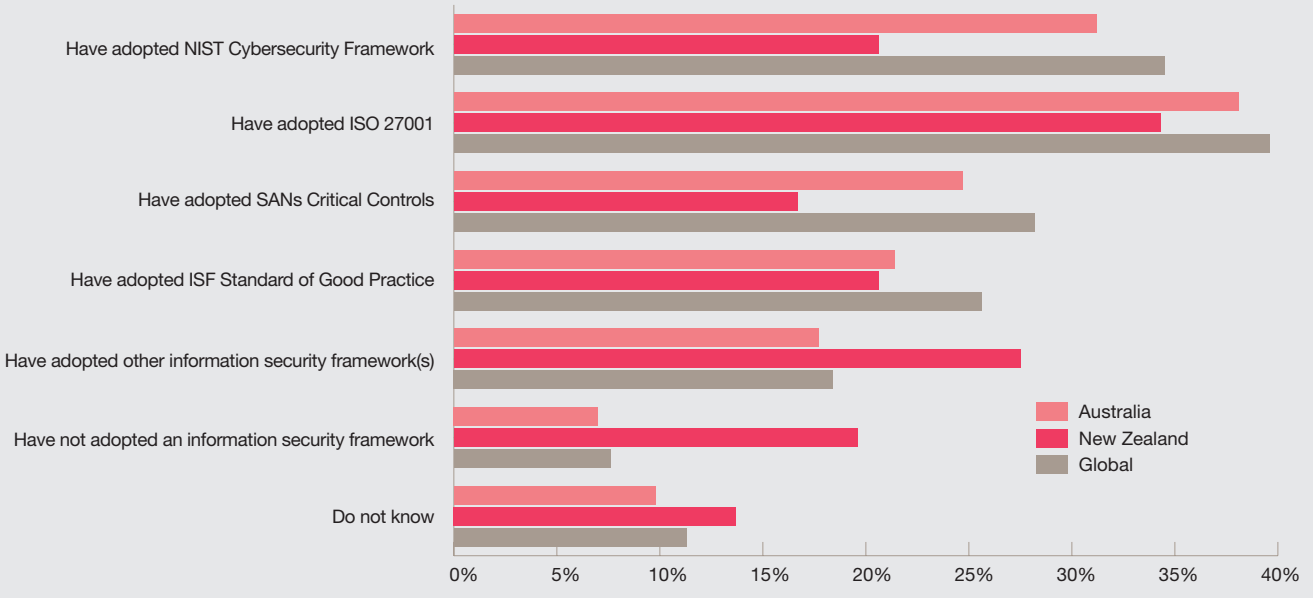
Most organisations have adopted a risk-based cyber security framework, which lays the foundation for an effective security program. As a result implementing these frameworks, organisations are better able to identify and prioritise security risks, as well as more quickly detect and mitigate incidents.

The two most frequently implemented frameworks are ISO 27001 and the NIST Cybersecurity Framework. However, in New Zealand many organisations have adopted another framework (see Figure 1), which is likely due to the New Zealand Government's directive for Government agencies to use a risk assessment method based on ISO/IEC 31000 and the New Zealand Information Security Manual (NZISM).

According to the Government Communications Security Bureau: "The NZISM is a practitioner's manual designed to meet the needs of agency information security executives as well as vendors, contractors and consultants who provide services to agencies. It includes minimum technical security standards for good system hygiene, as well as providing other technical and security guidance for government departments and agencies to support good information governance and assurance practices. It is consistent with a wide variety of risk management, governance, assurance and technical standards, including the ISO/IEC 2700x series, as well as IETF, OASIS, NIST and other recognised standards bodies."

At the core of these risk-based framework strategies is an investment in time to identify what information assets are important, then having the ability to detect, respond and recover should a breach occur.

Figure 1: Has your organisation adopted a risk-based information security framework such as the NIST Cybersecurity Framework, ISO 27001, Information Security Forum (ISF) Standard of Good Practice, or SANS Critical Controls?



What is my exposure? Punching holes in the perimeter security approach

The primary reason that pure prevention strategies no longer work is because today's business environment is highly dynamic and interconnected. There are simply too many avenues for information sharing – from suppliers and partners to customers and staff – meaning too many doors to effectively lock and police.

In our annual New Zealand CEO Survey, chief executives told us which technologies are strategically important for their organisation:

84% mobile for customer engagement

81% cyber security

74% cloud computing

73% internet of things

Understanding where exposure exists is about understanding an organisation's unique risks, and we know that these are on the rise in New Zealand. In our annual New Zealand CEO Survey, 84 per cent of chief executives told us that mobile technologies were strategically important for their organisation, 74 per cent said cloud computing and 73 per cent indicated that internet of things was strategically important.

Add to this, 50 per cent of CEOs have told us that they are looking at entering into a joint venture or strategic alliance this year, with the top reason being access to new customers.

As New Zealand businesses branch out overseas – an estimated 14,000 are now growing internationally – the exposure grows even more. In fact, 29.4 per cent of New Zealand respondents said that the adoption of a risk-based framework has better prepared their organisation to operate and compete across global markets.

And those organisations that will effectively manage their risk and maintain trust are the ones with strategies and frameworks to comprehensively manage information security and privacy. They will also understand:

- the security threats, intelligence and headlines that are relevant to them;
- what's important to their business and the risks to their operations and objectives; and
- real-time insights into their use of sanctioned and shadow digital services.

About one-third of New Zealand organisations have not adopted a risk-based security framework or don't know if they have adopted one, compared to 18.9 per cent globally. Of those who have adopted a framework in New Zealand, 52.9 per cent say they are better able to identify and prioritise security risks. More than half also say stakeholders better understand information security gaps and how to improve them.

Still concerning, however, is that more than 6 per cent of respondents in New Zealand don't know how a risk-based framework has impacted their organisations, compared to less than 2 per cent globally. This is likely because organisations here are still playing catch up to the rest of the world in terms of adopting these risk-based strategies and measuring the recent rise of cyber security investments. In this year's New Zealand CEO Survey, 81 per cent of respondents told us that cyber security is strategically important for their organisations (the second-highest behind mobile technologies).

Few organisations truly know how to establish metrics to measure the effectiveness of their security posture and to therefore judge whether the application of a framework and the deployment of controls is positively impacting the organisation or not.

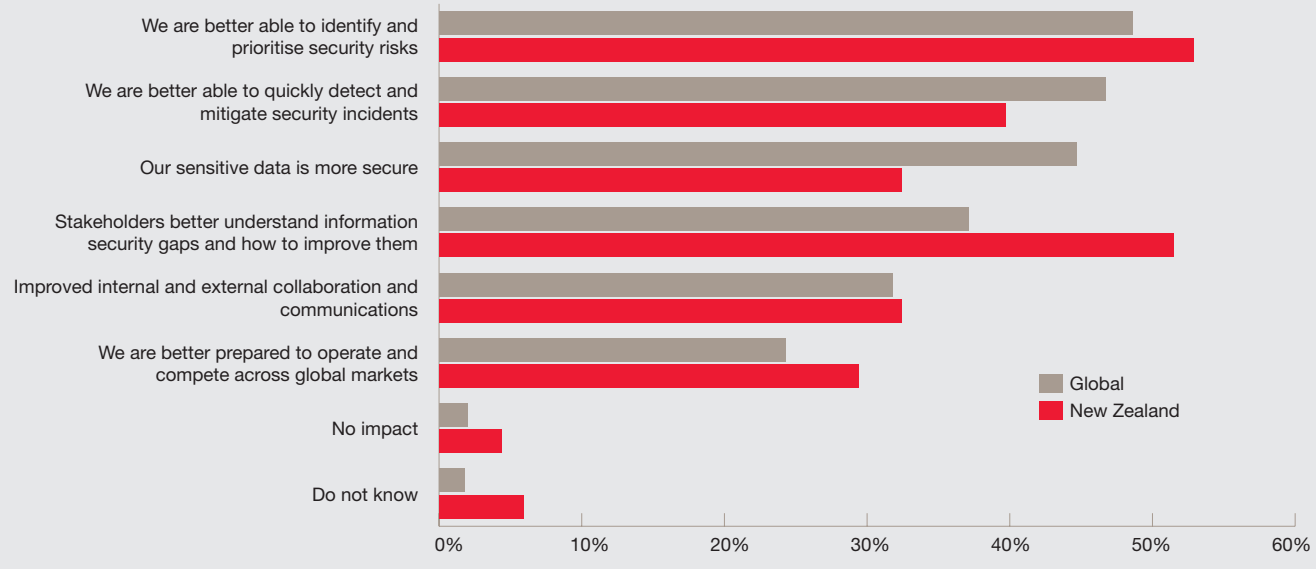
19.6%

of NZ respondents have not adopted a risk-based information security framework, compared to 7.6% globally.

35.1%

of NZ respondents classify the business value of data, compared to 48.2% globally.

Figure 2: What impact has the adoption of a risk-based framework had on your organisation?



Where is my data? The unsanctioned and uncontrolled use of cloud services

43.3%
of NZ respondents have a security strategy in place for the cloud.

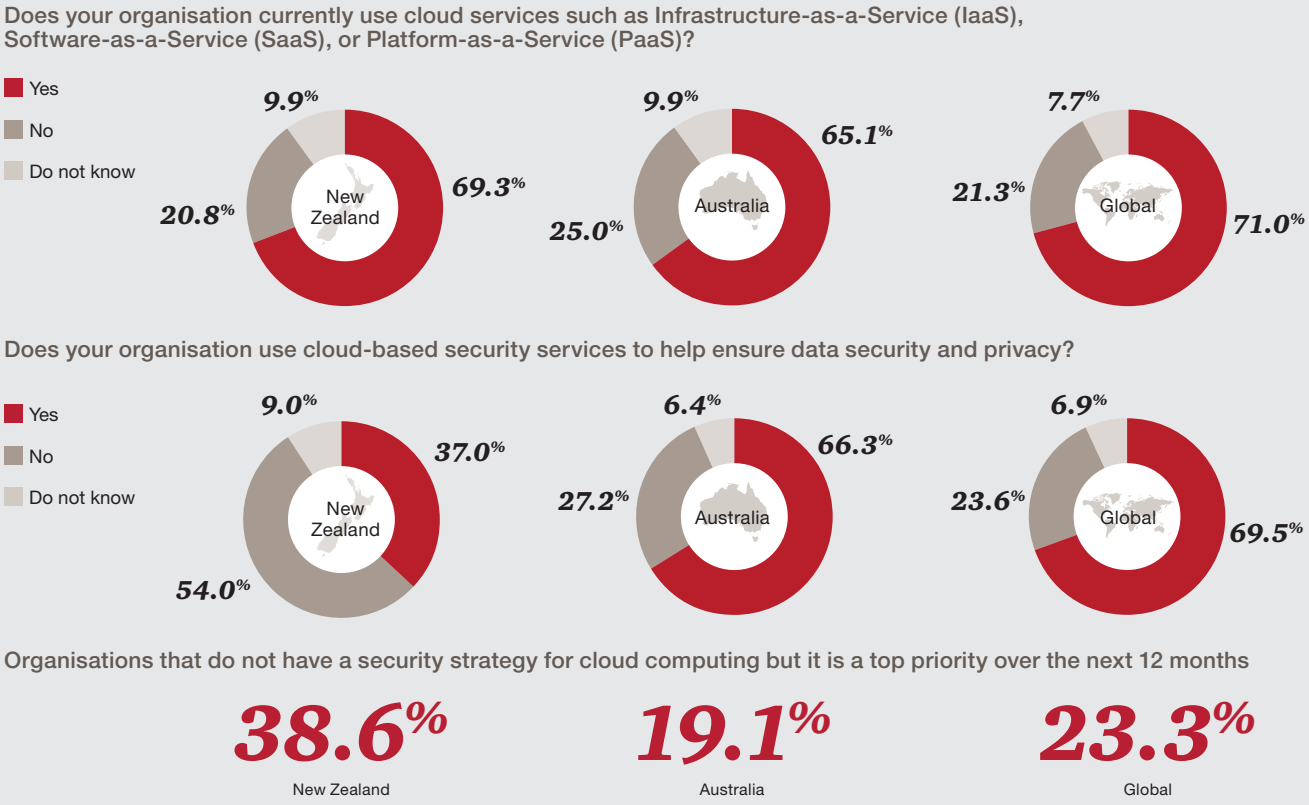
As mobile devices, cloud services and partnering among organisations continue to rise, so does the number of places that data can be accessed and stored. While 43.3 per cent of New Zealand organisations have indicated that they have a security strategy in place for the cloud, 40 per cent have mobile malware detection and 50.5 per cent use common identity protection – more than 40 per cent do not currently have an overall strategy that takes into account the holistic needs of the organisation.

What we know through our engagements with clients is that in New Zealand, Australia and across the globe, the gap between the business and the traditional IT department is widening. With ever increasing pressure to perform, business units – frustrated by rigid organisational structures – are circumventing internal blockades to achieve their own IT outcomes. This is known as "shadow IT." Shadow IT is not a new concept; IT departments have despaired for many years at users and business groups who download and install their own software to get the job done.

The recent explosion in shadow IT, however, has been dramatic. The culture of consumerisation within the enterprise – having what you want, when you want it, the way you want it and at the price you want it – coupled with outdated technologies and IT models has accelerated the adoption of cloud computing by business units and individual users.

Shadow cloud, the unsanctioned and uncontrolled use of cloud services, has now emerged as today's equivalent of the shadow IT problem creating both risks and opportunities for business. Through our own analysis in New Zealand and Australia, the average number of cloud services per employee is about 12, and these range from personal emails and storage services to social media and sites for illegal distribution of copyrighted and objectionable content. Policy is not the answer here because we found that virtually no business is complying with its own cloud policies.

Figure 3: About 70 per cent of New Zealand organisations say they use cloud services, and nearly 40 per cent don't have a security strategy in place but plan to make it a priority in the coming year.



This reinforces the need for organisations to identify the business value of data and what is critical for their own operation. While 48.2 per cent of organisations globally say they classify the business value of data, only 35.1 per cent of New Zealand respondents indicated that they do so. Additionally, big data is not top of mind for New Zealand organisations where only 26.8 per cent have a relevant security strategy, compared to 44.8 per cent globally. This means not only are New Zealand organisations not focused on protecting the data, but they also aren't looking to leverage this important asset to its full potential.

This year's Global State of Information Security Survey illustrates that organisations in New Zealand and Australia are slightly below the global norm in their adoption of cloud services (Figure 3) and well below the global average in their use of cloud-based security services to protect information.

Whether or not organisations formally recognise it, the consumer culture driving information technology consumption is a modern enterprise reality that is here to stay. Organisations willing to work with their business units, individuals and cloud providers to better understand the levels of activity, risks and benefits will ultimately gain from their efforts.

Who has access? Advanced authentication and third-party connectivity

28.4%

of NZ respondents use biometrics as an advanced authentication technology, compared to 58.9% of respondents globally.

The question of 'who has access and to what' is about the management of authorised users, such as staff, partners or service providers. This is where it's important for organisations to understand the role of advanced authentication in their strategies.

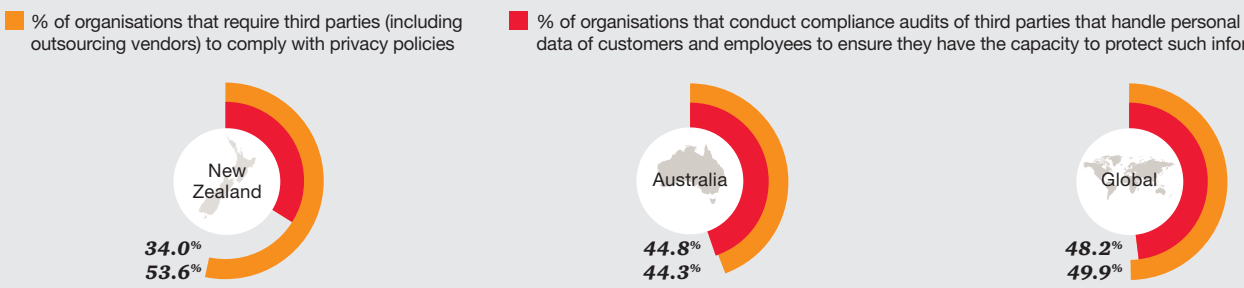
In New Zealand, identifying who has access to an organisation's information is one of the most challenging information security problems today. When an employee, supplier or partner uses business-to-business connectivity, mobile devices or the cloud, it breaks the historic model of keeping information in-house and stored within a single organisation and single security domain controllable by the organisation.

Most survey respondents globally use some form of advanced authentication, such as software tokens, hardware tokens, cryptographic keys and biometrics. In New Zealand, many organisations have adopted at least some of these measures, but still lag significantly in the uptake of biometrics – fingerprints, retina scans, facial recognition, for example – and smartphone tokens.

Organisations that use these advanced authentication methods are seeing a range of benefits, such as improved customer or business partner confidence in security and privacy capabilities, improved customer experience, enhanced fraud protection and more secure online experiences.

Third-party connectivity will continue to play a key role in New Zealand as many businesses are relatively small on a global scale and choose to partner with other organisations to gain access to new geographies or customer bases. However, it's concerning that only 28.4 per cent of New Zealand respondents say they conduct compliance audits of third parties (that handle personal data of customers and employees) to ensure they have the capacity to protect such information. This is compared to 48.2 per cent globally.

Figure 4: While more than half of New Zealand respondents say they require vendors and partners to comply with privacy policies, only about one-third conduct compliance audits.



Have I been breached? … and what do I do?

28.0%
of NZ respondents with a security incident in the past year suffered a loss or damage to internal records.

25.6%
saw their brand or reputation compromised.

22.0%
don't know how their organisation was fully impacted.

18.3%
suffered financial losses.

Many New Zealand organisations still operate under the assumption that they won't be breached. The lack of regulation for data protection, mandatory disclosure in the event of a data breach, and formal mechanisms to collect meaningful data on New Zealand incidents is why this myth persists.

So while anecdotal evidence and the anonymised feedback of this survey indicates the number and impact of cyber incidents continues to rise, much still flies below the radar in New Zealand. Without meaningful regulatory and structural changes here to encourage and drive the right behaviours, this disturbing trend is unlikely to change given the ongoing uptake in digitisation, cloud and mobile technology.

However, some organisations in New Zealand are waking up to this realisation. This year our annual CEO Survey showed that cyber security, including the lack of data security, was third-highest threat to business growth for New Zealand's chief executives. This year, 66 per cent of CEOs cited this as a top-three threat, up from just 40 per cent in 2014.

While C-suite and boardrooms are shifting their focus, they are falling behind in global trends in cyber security spending. Nearly 40 per cent of New Zealand respondents have no plans to adopt big data analytics to model for and identify information security incidents, compared to 11.3 per cent globally and 13.9 per cent in Australia. Of those who adopted it globally, 61.3 per cent say it has improved understanding of external security threats and 48.6 per cent say it has improved understanding of internal threats.

Ideally, any organisation (big or small) should have a cyber response plan and be ready to initiate it. However, we have found that many organisations in New Zealand don't have one or they view a security breach as any other technology incident. Our experience and the survey tells us cyber incidents are markedly different in their causes, impacts and treatments. We know and have seen that in today's digital landscape, the speed of detection of a cyber incident and the way an organisation responds and recovers can be the difference between staying in business or becoming another statistic.

Three critical success factors of navigating a cyber incident

Experience: In the middle of an incident, there is nothing like the calming influence of someone who has done this before. If you don't have it, know where to go for it.

Decision-making: Having the ability to get relevant information to people who can make risk-based calls quickly.

Communication: Recognising the widest possible stakeholder group and owning the messaging around the incident is critical – and it's one of the biggest mistakes organisations can make if they don't get this right.

How do I know? Levels of confidence are dropping in New Zealand

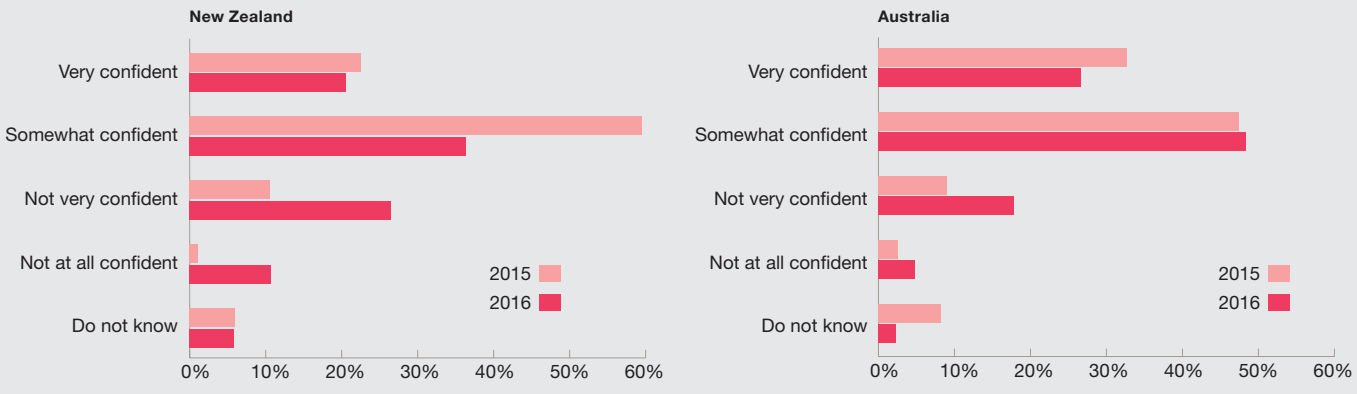
How do I know if I have invested effectively, my data is safe, have done enough or whether I am really managing my risk? These are the big business questions that New Zealand organisations ask every day – and the data shows that confidence is down.

Last year, 83.3 per cent of New Zealand respondents were confident or somewhat confident that their organisations' information security activities were effective. This year, 64.7 per cent are confident or somewhat confident. While confidence is dropping, it likely represents a more accurate picture of real versus perceived risk. As more organisations adopt risk frameworks, they are gaining a better understanding of their risks and what they need to do to manage them.

Survey data in recent years in New Zealand has shown that high confidence doesn't necessarily match the actual measures taken to secure information. The reasons for this, at least anecdotally, is that some organisations say no one has told them that something is wrong so they choose to believe there is no issue. Another reason is that many New Zealand organisations trust their suppliers and believe that they will simply do the right thing when needed – despite the absence of or even the specific exclusion of security obligations from contractual agreements. They also assume that because they have spent money on security technology, then it must have resulted in improvements.

When called upon to conduct breach assessments in New Zealand, we have identified a significant issue about 90 per cent of the time. What is alarming is that our data indicates that two-thirds of breach notifications now come from outside of the organisation. The reality is until you have invested time in understanding your current state – and that this critical information is driving your security activity – you can never truly know.

Figure 5: How confident are you that your partners' and suppliers' information security activities are effective?



Conclusion
Flourishing in tomorrow's interconnected world

In the coming year, NZ respondents are making the following safeguards a top priority for their organisations:

43.4%
a programme to identify sensitive assets

42.2%
security strategy for mobile devices

41.0%
classification of business value of data

41.0%
establish security and baseline standards for third-party vendors, suppliers, and external partners

Advanced and enhanced information security practices will not only enable organisations to better defend against cyber threats, but they can also help create competitive advantages and foster trust among customers and business partners. This is particularly important in New Zealand, where we tend to be highly trusting.

In addition to the focused risk framework approach, coupled with new technologies and processes, many organisations are emphasising the people side of the cyber security equation. Across the globe, organisations are expanding the roles of top security executives, CEOs and boardrooms. In New Zealand, we are finding an enthusiastic interest from boards and executives for more education and information about their organisations' information security activities.

There is no magic bullet for effective cyber security. It's a journey towards a culture of security, not a solution in and of itself. It is a path that starts with the right mix of technologies, processes and people skills.

The organisations that will flourish in tomorrow's interconnected world are those which recognise that good cyber security is good business. Effectively they understand that by managing their risks, they can use digital technologies and their information assets to realise opportunity with confidence.

Want more data?

New Zealand organisations' investments in safeguards to defend their ecosystems against evolving threats

- 50.5% Employee training and awareness programme
- 81.4% Malware or virus-protection software
- 25.8% Behavioural profiling and monitoring
- 56.7% Vulnerability assessments
- 35.1% Classify business value of data
- 36.1% Programme to identify sensitive assets

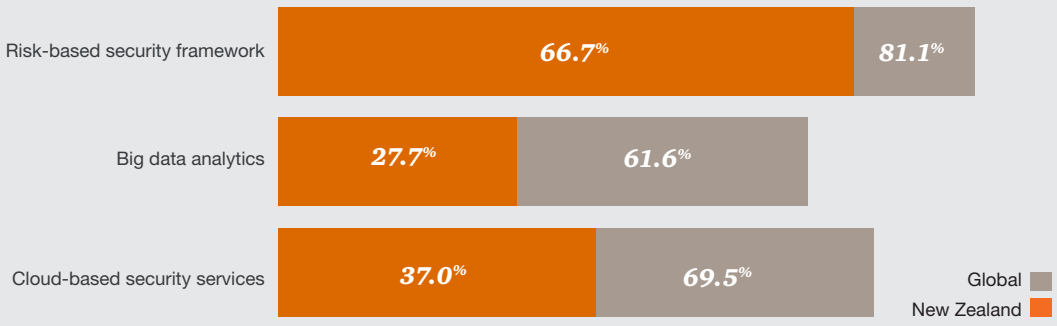
42%

of New Zealand organisations that have experienced a security incident in the past year say the source was a current employee, compared to 33.6% globally.

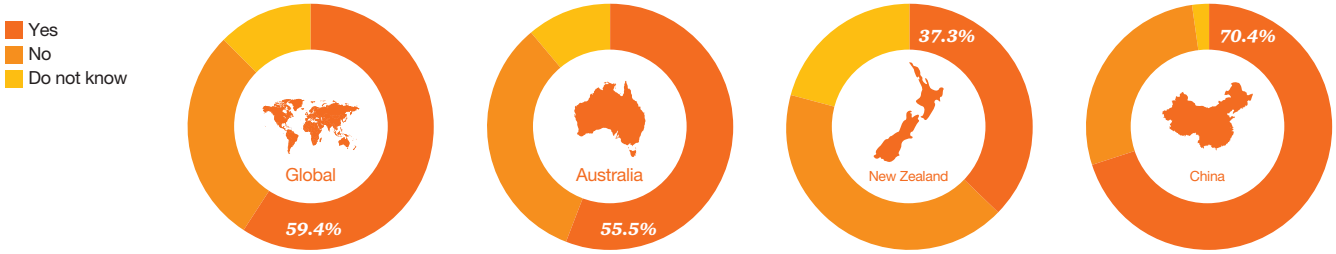
25%

of New Zealand organisations with cyber insurance made a claim in the past year, compared to 50.4% globally.

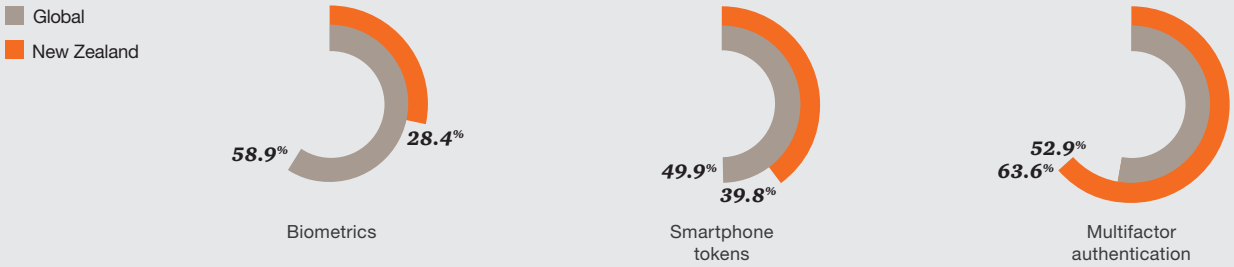
Organisations that have adopted these initiatives to improve security and reduce risks

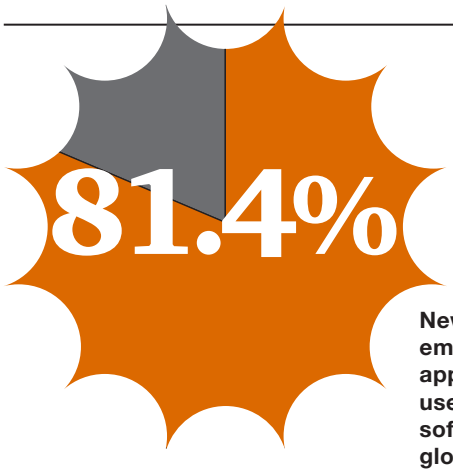


Does your organisation have cyber insurance that protects it from theft or misuse of electronic data, customer records, etc?



Which of the following advanced authentication technologies does your organisation currently have in place?





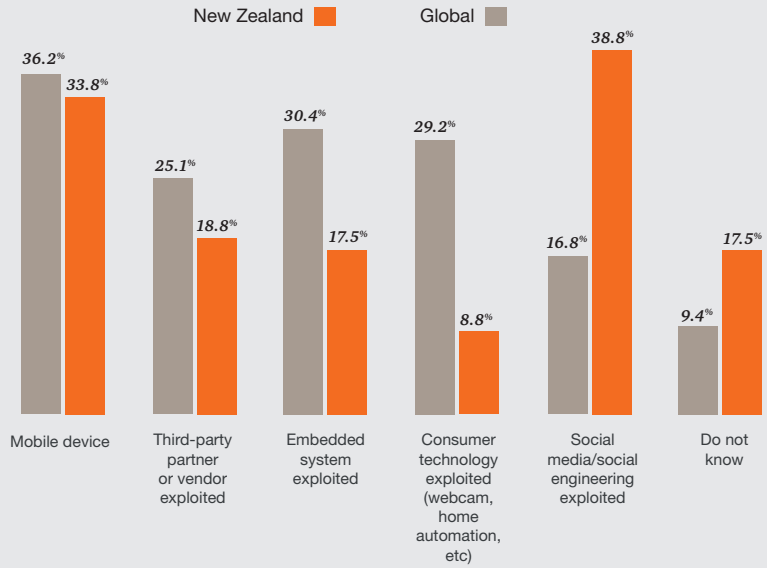
New Zealand respondents are still embracing the perimeter security approach with 81.4% saying they use malware or virus-protection software, compared to 57.8% globally and 47.9% in Australia.

of New Zealand respondents say they have no plans to adopt a programme to identify sensitive assets.

New Zealand respondents are much less confident this year that their organisations' information security activities are effective. Last year, 83.3% of New Zealand respondents were confident or somewhat confident, compared to just 64.7% this year.

They are also less confident in the security activities of partners and suppliers. Last year 82.1% of New Zealand respondents were very or somewhat confident, compared to 56.9% this year.

How did security incidents occur in New Zealand and across the globe?



Get in touch

Adrian van Hest
Partner
T: +64 4 462 7109
E: adrian.p.van.hest@nz.pwc.com

Steve McCabe
Partner
T: +64 4 462 7050
E: steve.c.mccabe@nz.pwc.com

Richard Tims
Director
T: +64 9 355 8705
E: richard.d.tims@nz.pwc.com

pwc.co.nz

pwc