Cyber security in a digital business world

Putting security at the centre of New Zealand organisations

The Global State of Information Security Survey 2017

68%

of cyber security leaders will invest more in security as their business model evolves.

44%

are using managed security services

21%

report that suppliers and business partners were the source of a cyber attack in the last 12 months

pwc

www.pwc.co.nz/gsiss2017

Contents

Executive summary

The megatrend of technological breakthroughs is here to stay. It's already reshaped entire industries and now every organisation is facing a very dynamic risk profile as they look to realise the many opportunities that technology presents. The rise of digital business models also means that every New Zealand organisation is exposed to an evolving level of digital risk, either from customers and employees or from relationships they have up and down their supply chain.

Digital business models aren't just limited to internet businesses either – we've seen in recent years a complete transformation in both front- and back-office functions. In fact, it's often these back-end functions where the greatest prize is for cyber attackers.

In New Zealand we are experiencing the natural growing pains that come with the widespread adoption of cloud computing, big data, social media and mobile technologies. None of these technologies are inherently risky in themselves, but that can change given certain contexts and settings. What's more, the next generation of wearables, along with the Internet of Things (IoT) more broadly, will further transform the way we approach cyber security and privacy.

These trends have come through clearly in our research. While we've seen local businesses continue to invest in cyber security, we still lag behind comparable economies. What's more, our spending on cyber security is less aligned to business functions and value than overseas firms and isn't as focused on what specific controls work best for the organisation's critical information and systems.

The adoption of cloud is driven be the ability of businesses of any size to leverage efficiencies, scale and functionality that was previously beyond their reach. Which is why our adoption of this technology is well ahead of the rest of the world. The need now is for kiwi businesses is to ensure their security and privacy efforts expand at the same pace as their broader business and digital activities.

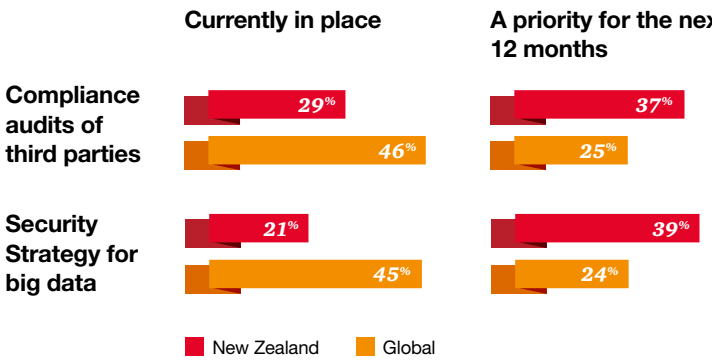
In every organisation, context is key. In order to invest effectively, organisations have to take a personalised approach to their cyber security, one that is specific to their business needs, their existing digital ecosystem and their relationships with business partners.

This is the first of four white papers we will release over the next 12 months that explore different angles of the 2017 Global State of Information Security Survey. I'd like to thank all of our New Zealand respondents who took part in this year's survey – the 19th we have published – and I hope you enjoy our extended coverage of this important issue.

Adrian van Hest
Partner and Cyber Practice Leader

The state of cyber in New Zealand

The cyber security response from businesses



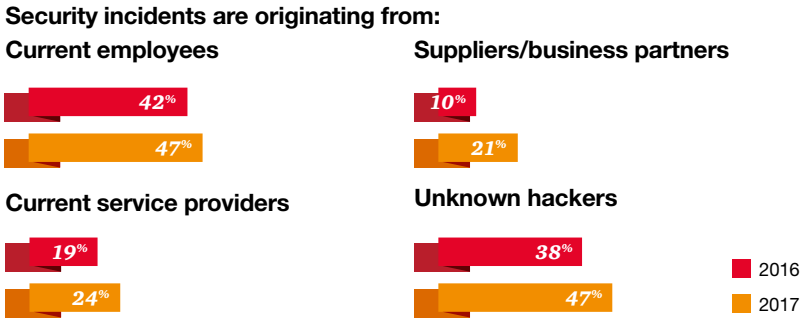
The digital business ecosystem is reshaping cyber security in New Zealand:

57% are *investing more in security*

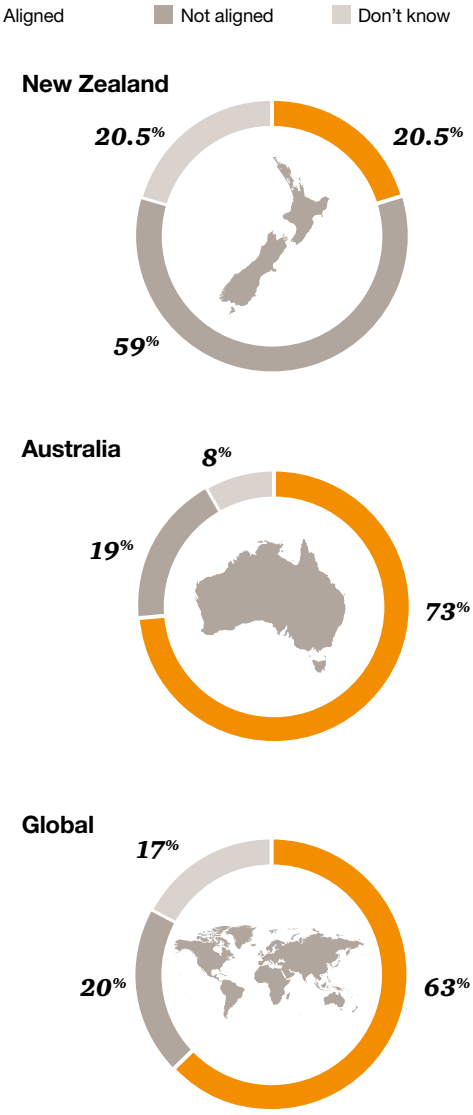
68% will invest in *new security needs* related to *evolving business models* in the next 12 months

56% will invest more in *improved collaboration between business, digital and IT* over the next 12 months

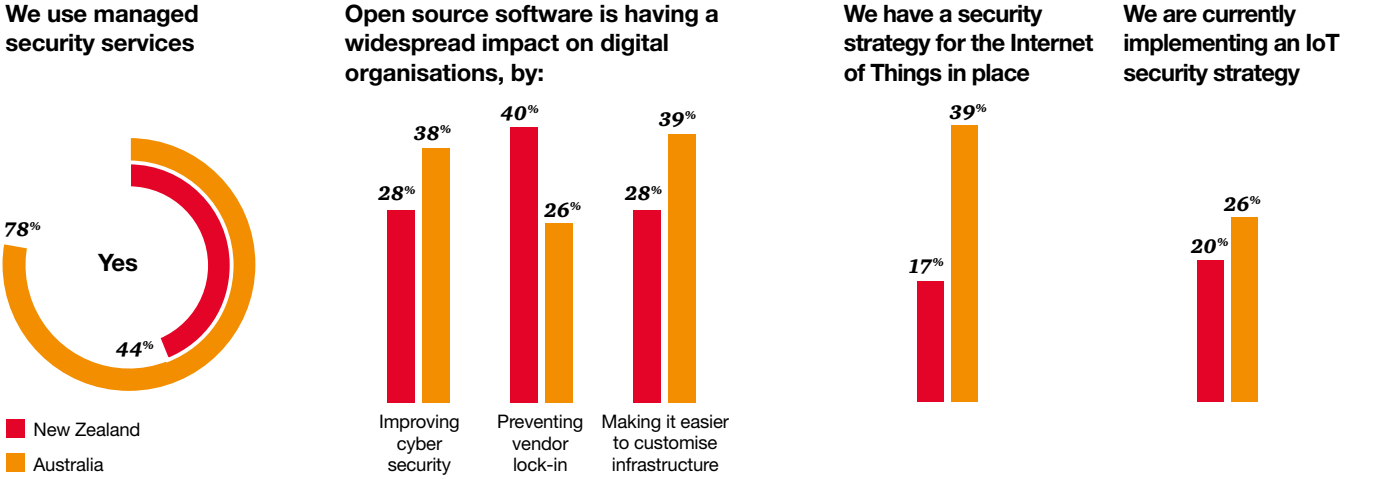
Across the board, New Zealand companies are responding to a greater range of threats



The majority of cyber security spending isn't aligned with business revenue:



How New Zealand's digital businesses compare to Australia's



The cyber challenge of digital business

How companies think about their digital assets is changing. No longer a matter of isolated IT assets, companies are now developing complex, multi-faceted digital ecosystems. There's now no aspect of a business's operations that can't be translated into a digital equivalent, allowing businesses to lower operating costs, raise employee productivity and scale their operations quickly. The result is a digital business presence that is not only larger than ever but also has increasingly blurred lines between a company and its suppliers, not to mention the personal presence of their customers and employees.

The ability of cloud platforms to deliver functionality, storage and processing power, all with no significant capital investment has played a huge role in creating this ecosystem, providing a framework for businesses to go truly digital. However rapid adoption and simplistic assumptions about how it works and just what is secure means there is often quite a gap between an organisation's assumed and actual level of risk.

This is proving especially true in New Zealand, where cloud adoption is among the highest in the world. In fact, 90 per cent of our respondents identified they are using some form of cloud computing model, either public, private or hybrid. Alongside cloud services, companies are also moving into other foundational elements for their digital presence, from big data and mobile devices through to social media, all of which are creating new data concerns. Despite this, Kiwi companies are half as likely as the global average to have a big data security strategy (21 per cent compared to 45 per cent).

Cloud computing has helped to underpin another hallmark of the digital business: Bring Your Own Device (BYOD) policies. While these policies represent a valuable way for companies to make work more flexible, they also further blur the boundaries of a company's digital footprint. In New Zealand, companies are struggling with the security implications of BYOD, ranking below the global average for having a security strategy in place for personal devices used in the workplace.

New Zealand firms are more likely to develop a security policy in-house, rather than outsource it to a third party (8 per cent locally compared to 27 per cent globally and 32 per cent in Australia).

As a result, companies are running the risk of saddling themselves with legacy systems and practices that can't protect them against new risks, that don't scale up as the business expands and that aren't based on industry best practice.

Of course, outsourcing isn't the only method for digital businesses to improve their cyber security. Relying on open-source technology, both for general business solutions and also to protect the business's data, is an increasingly popular global solution.

Open-source has certainly caught on in recent years, with 40 per cent of New Zealand businesses using open-sourced software to avoid vendor lock-in, while allowing them to easily undertake new IT projects. However, compared to our global respondents, New Zealand organisations are considerably less likely to use open source technology or recognise the opportunity it offers to improve their cyber security efforts. This lack of awareness about the potential applications and benefits of open-source software represents a missed opportunity for New Zealand's public and private sectors, although this may be an issue of scale.

Safeguarding digital business

In this digital ecosystem companies have to be mindful that every supplier and service provider is a potential avenue for a cyber attack, and that they need to take appropriate steps and hold them to account for any breaches.

Data privacy as a competitive advantage

We now generate more data than ever before across multiple connected devices. More importantly, it has become easier than ever for people to access that information, either legitimately or as the result of a cyber attack.

For sensitive data, the risk posed by a cyber attack has morphed from one that is purely operational to one that segues across a company's brand, reputation, business continuity planning, staff and customer relationships. As a result, data privacy is increasingly being seen internationally as a key competitive advantage – something that customers and clients now expect.

New Zealand organisations are just now realising that they are no longer seen as the victim in the event of a data breach, but regarded as someone who has abused their client's trust in them. From a customer's perspective, data privacy isn't an optional extra, it's a core component of their willingness to purchase from a business. They are also more willing than ever to hold organisations to account for breaching their privacy. Despite this, local companies are struggling to put safeguards in place to protect the data they gather. In New Zealand, only 42 per cent currently inventory personal data from customers and employees, 11 percentage points behind the global average.

Having qualified staff is one part of the puzzle for digital businesses, the other is the third parties that a business partners with. Only half (48 per cent) of New Zealand businesses require the third parties they work with to comply with their privacy policies. The message here is clear – while privacy policies are an important first step in protecting customer data, these standards cannot be implemented in isolation - they have to be applied across every aspect of an organisation's operations. Effectively this demands a cultural shift across the organisation, equivalent to the strides New Zealand is making in health and safety.

The regulatory imperative

To date, regulators have been playing catch-up with changes in our ability to generate and capture data. Despite this, overseas regulation has continued to evolve and digital businesses are now recognising the need to not only conform to the data privacy requirements of their home market, but also those of any overseas territories they are working in. This is where New Zealand's lack of regulation and enforcement hurts us as a destination for digital business.

Sixty-four per cent of our Kiwi respondents said the reason they have a privacy function is to maintain compliance with regulation. That's considerably more than the global average (50 per cent) and that of Singapore (56 per cent), a regional economy roughly the same size as New Zealand.

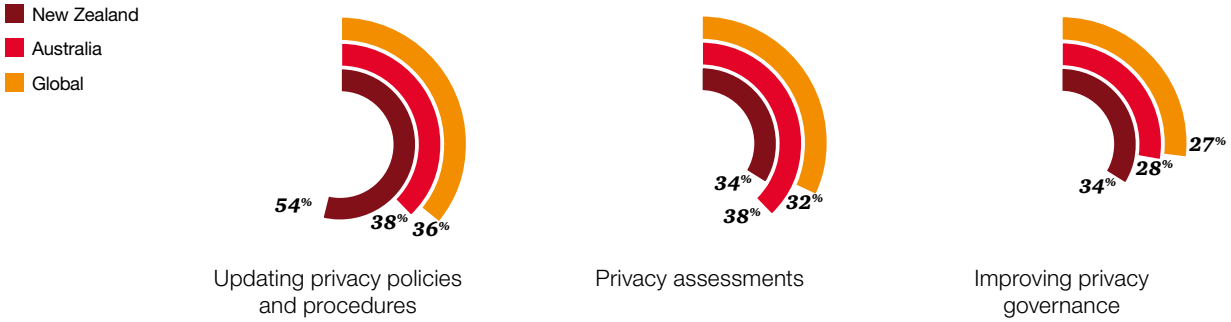
What's also interesting is what New Zealand companies aren't focusing on. Many global respondents (31 per cent) identified that their privacy function allows them to get more use out of the data they collect, through better marketing initiatives, for example. Only 26 per cent of our local respondents identified the same benefit, lower than both Australia and Singapore. In these countries, privacy is seen as a way to stand out and appeal to customers who are increasingly protective of their data – in New Zealand it's treated solely as a question of compliance.

Companies collecting information globally are facing an increasingly complicated regulatory environment as different jurisdictions introduce legislation to protect their citizens' data. The European Union, South Korea, Hong Kong and Singapore have all introduced new data protection regulations – reflecting a greater awareness across New Zealand's major trading partners of the importance of data security. While we might like to think of digital businesses as being borderless, the increasing complexity of cyber security legislation is changing the way businesses manage privacy concerns.

By comparison, New Zealand's lack of mandatory disclosures and reporting around data breaches puts us behind many of our major trading partners. There is a long-term risk that, without updates to local legislation, New Zealand businesses are unprepared to operate in global markets, while the country also becomes less attractive for companies looking to do business here.

Responding to changing regulation

Among the key responses NZ organisations are taking to privacy regulations, these are three of the most popular:



Finding new solutions to old cyber concerns

Awareness of cyber security has been growing year-on-year, and organisations in New Zealand are now more aware than ever of how exposed they are to cyber risks and how their operations will be affected if (or when) they are the victim of a cyber attack. The next challenge that many local organisations are now struggling with is translating high-level awareness into a deeper understanding of the breadth and depth of risks their organisation is facing.

Globally this is happening. The conversation is changing to focus less on knee-jerk reactions and more on establishing the frameworks and architectures that can reduce a company's long-term exposure to cyber crime. These companies have a holistic cyber strategy to identify, protect, detect and respond to the risks they face. Driving this approach is a leadership team who aren't just aware of cyber risks but who understand the breadth of possible threat actors and are actively championing cyber security.

Locally, companies will have to keep up with this shift and invest in the same best-practices that we are seeing internationally. New Zealand businesses that haven't already implemented a data use framework will have to do so, while those that have will need to update the framework as their digital footprint changes with new technologies. This process will allow them to address any redundancies in their IT architecture.

Likewise, the growth in cyber attacks from employees and business partners underscores the new areas of focus for local companies. Local organisations now have to develop a collaborative strategy that crosses both organisational silos and the traditional "perimeter security" that stood between a company and its third-party service providers. To achieve this, 56 per cent are looking to increase the collaboration that occurs between business, IT and digital. Context is key here – a successful strategy won't be an out-of-the-box solution, but carefully tailored to match the organisation's structure and digital presence.

Digital organisations will have to invest more into managing the data lifecycle. In New Zealand, only 39 per cent of our respondents will be investing in an accurate inventory of how personal data is collected and used.

Finally, New Zealand firms have to be more selective when it comes to the third-parties they work with. The percentage of respondents experiencing security breaches from suppliers has doubled in the last year and will keep growing in the future. Formulating a response has to start with the context – where their data is and who (both within the business and externally) has access to it. From there, they can begin to develop a range of advanced security techniques that will allow them to prevent, detect and recover from a cyber attack, regardless of its origins.

Future opportunities:

Bake a cyber security framework into new digital initiatives: Retrofitting digital infrastructure with security measures will never be as effective as building these features in from the start.

Invest in detecting and responding to new types of cyber attacks: Local companies are over-reliant on penetration tests compared to the rest of the world and have to diversify into more advanced tools like risk-based authentication/authorization, while also addressing the risk posed by staff and suppliers.

Move away from solely in-house cyber security: New Zealand firms rely more on in-house measures than their global counterparts. Outsourced expertise, open source security software and scalable third-party tools can all provide a more effective security solution – and are all measures that overseas firms are actively pursuing.

Be ready to respond. Success or failure in cyber security comes down to how well companies respond after a breach.

Get in touch

Adrian van Hest
Partner and Cyber Practice Leader
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

Methodology

The Global State of Information Security Survey is our annual cyber security publication, polling 97 cyber security specialists and decision-makers from across New Zealand as part of a global survey of more than 10,000 experts in this area. This year's findings will be published as four whitepapers throughout the 2017 financial year. The results are published in conjunction with CIO Magazine.

pwc.co.nz

pwc

© 2016 PricewaterhouseCoopers New Zealand. All rights reserved. 'PwC' and 'PricewaterhouseCoopers' refer to the New Zealand member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.