Who's managing your identity?

The cyber risks of our digital business world

pwc

pwc.co.nz/gsiss2018

Keeping identity secure in a digital society

Our lives have become enmeshed in the digital ecosystem that makes up our modern society. Our identities are no longer just defined by our personal traits, but by the ever-growing amount of data that we now generate online. For companies charged with storing and protecting this data, while still delivering on a seamless customer experience, understanding and managing identity has never been more important.

As our society has gone digital, the nature of cyber security has changed as well. It's no surprise that New Zealand businesses are now running into the cyber risks that come with new business models. Cloud computing and mobile devices bring with them new risks – not because the technologies are unsafe, but because they require companies to take a different approach to the way they manage cyber security.

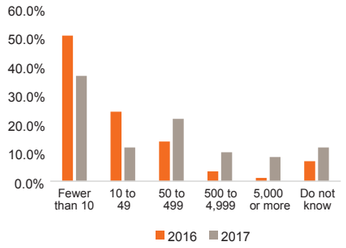
Yesterday's cyber security practices aren't suitable for this new world, especially as the number of incidents increases every year. As yesterday's emerging technologies become the foundations for a new generation of products and services, security at every level only becomes more important. Like any complex structure, our digital ecosystem is only as strong as its weakest link.

What's working? (And what isn't?)

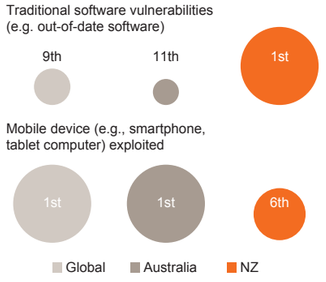
It's no surprise that investments in identity management and cyber security have continued to increase, especially as the number of attacks has gone up. Last year, half our survey respondents said they'd had up to 10 cyber attacks. That's dropped to only a third this year.

Is your organisation's cyber spending aligned with revenue?

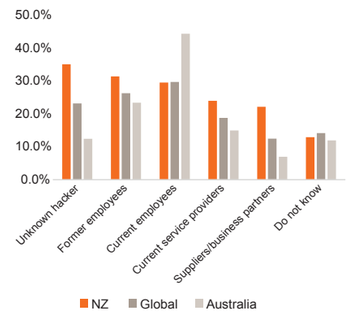
What is the number of security incidents detected in the past 12 months? (New Zealand)



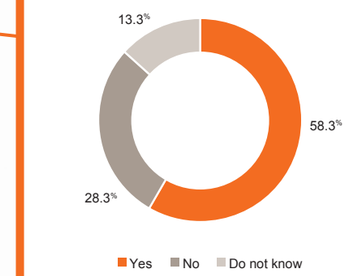
What are the most common causes of security incidents?



Where did the cyber incident originate?



Does your organisation have cyber insurance? (New Zealand)



However, here in New Zealand we're still underinvesting when compared to our global counterparts in identity management. The average global company is spending almost US$1.5 million more on security each year than their NZ counterparts ($5.1 million vs $3.7 million). Although up on last year, just half of New Zealand businesses are aligning this security spend with revenue.

Perhaps the biggest challenge, though, is the lack of awareness around digital identities and the role they play in underpinning many of the bigger transformations companies are embarking on. As businesses move to the cloud and to mobile, digital identification acts as the cornerstone.

Overseas, companies are already experiencing the challenges of poorly aligned security – with mobile the most common source of cyber incidents. Locally, we're still trailing in this area, but as more businesses move to mobile, it's only a matter of time before we catch up.

How are we comparing internationally?

Here in New Zealand, we're a high-trust society. While that certainly helps us maintain an open economy, it's also putting our companies at a disadvantage in the world of cyber security. Our digital society is increasingly globalised, and the approach companies are taking to identity management locally is being measured against global standards, from the EU's General Data Protection Regulation (GDPR) to increasingly complex Chinese cyber security laws. Despite this, only half our respondents have taken any action to understand their exposure to the GDPR. New Zealand's attractiveness as a connected economy will depend on local businesses understanding the changing global cyber security landscape and taking steps to reduce their exposure if they want to stay connected to global marketplaces.

Compliance is just the tip of the business benefits of effective identity management. It's the starting point for our digital, mobile and cloud-based society. Without effective identity management, any further efforts to transform cyber security practices here in New Zealand are going to be an uphill struggle.

The known unknowns

Sources of threats are just one part of the security puzzle that comes with a digital society. Beyond the 'how', we have to look at 'who' is a threat if we're going to understand the state of cyber security in New Zealand in 2017 and beyond.

We know the vast majority of our respondents have had at least one cyber attack in the last year, so we asked who was responsible for the attack. In New Zealand, the largest category was the catch-all "unknown hacker", followed by former employees. Globally, we saw a lot more certainty – current and former employees were by far the most common sources of a cyber attack. Ultimately, it's people who are the greatest cyber risk – whether it's an employee, a contractor or a worker within a partner organisation.

As our society becomes increasingly digital, understanding the breadth of possible threats is certainly important – we saw the number of security breaches coming from partner organisations double in last year's survey, a number that's remained high this year and above our counterparts in Australia.

Transforming cyber security

We can't rely on yesterday's cyber security practices to keep organisations secure. The need for more robust processes and policies has never been greater. What's changing, though, is that cyber security is no longer an issue for IT departments, it's becoming an issue that cuts across our entire digital society.

The popularity of cyber insurance

Cyber insurance has certainly come of age – it's a popular choice and we're seeing many New Zealand businesses take this option. Over half our respondents now have a policy (58 per cent), slightly behind Australia. What we're now seeing though is insurers taking the front foot and expecting clients to proactively manage their cyber risk. It won't be long before New Zealand's cyber insurers are demanding companies have their cyber security processes independently verified to confirm they're maintaining best-practices.

Forget talking tools, start talking outcomes

Responding to this changing world requires a shift in mind-set from today's business leaders. Investing in cyber security is a great start – but more resources alone won't transform the way we approach cyber security. We still see a lot of organisations that treat cyber as a technical issue, not a business one.

We're also seeing too many organisations that are putting money into cyber but can't first identify the core risks they are facing and the assets they are trying to protect. There's a lot of focus on the infrastructure involved, but much less on the strategy that sits behind it. Without this thinking, we can't successfully deliver on the full opportunity that cyber security presents.

Ultimately, we have to transform cyber security by being laser focused on the risks involved. Companies that stay competitive in our digital landscape aren't just blindly trusting that their business and customer data will stay secure. It's no exaggeration to say that building and maintaining trust is going to be the greatest differentiator for New Zealand businesses in our digital society. Now's the time to start taking that seriously.

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

Campbell McKenzie
Director
T: +64 9 355 8040
E: campbell.b.mckenzie@nz.pwc.com

pwc