The digital identity imperative

Five reasons why digital identity is the key to reinvention, for New Zealand businesses

pwc

What is digital identity?

Essentially, digital identity is proof of who you are online. It involves using technology to share pieces of personal or organisational information. Sharing this information (or 'attributes') digitally allows users to access services and make transactions online.

Why is digital identity so important?

Following the COVID-19 outbreak and an increase in ransomware events, organisations worldwide were forced to rapidly adapt to new ways of working and new business models. For most, it was a parallel challenge of maintaining a remote, productive workforce while rapidly establishing or scaling digital channels to reach and service consumers.

IT and digital departments responded to unprecedented demand for remote access as well as demand for maintaining systems and processes to support staff with the efficient delivery of work. With these challenges, it quickly became apparent that the core digital identity questions of 'who are you?', 'can you prove it?' and 'what are you entitled to access?' were fundamental to a successful, efficient and effective response.

Those organisations with mature digital identity capabilities found themselves able to onboard and offboard employees instantly, grant and remove access to information and applications, and put additional controls in place to safeguard resources from an even greater risk of uncontrolled distribution.

They were also able to rapidly provide solutions that allowed customers to self-provision secure access to products and services. They could get to market faster than their competitors using channels that had previously been serviced in-person or that required a degree of face-to-face contact.

Those without good identity management were still able to deploy a remote workforce but many admit they were unable to do so securely.[1] Those still operating perimeter-based models, where internal identity and access was a free-for-all, were suddenly exposed to increased risks. Not least because employees and suppliers worked remotely from unknown devices with unmonitored identities that could access almost anything.

So in our current and future reality shaped by this global pandemic, the management of digital identity and the identity landscape is more important than ever. Here are our five reasons why digital identity is key to reinvention.

1 https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/pwc-covid-19-ciso-pulse-survey.html

Five reasons why digital identity is the key to reinvention:

1. It's the grease in the organisational wheels

Controlling your identities makes everything run smoother and helps you move faster.

2. It's a transformation enabler

A sound identity management structure makes it far easier to integrate systems and transform.

3. It's the foundation of securing your critical assets

Identity and access is always a significant source of threat and risk. The pandemic has only increased this threat as organisations have rushed to deploy a remote workforce and service more customers online.

4. It fosters innovation and confidence

Without confidence in identities, systems and access, innovation can be stifled by overzealous reactions to regulation and compliance.

5. It's the only future identity

The New Zealand Government is embarking on a transformation programme for digital identity that recognises the need to modernise and scale efforts to be fit for future growth.

We dive deeper into each of these reasons, in the following pages.

1 Digital identity is the grease in the organisational wheels

Controlling your identities makes everything run smoother and helps you move faster.

Consider the time it takes to make a new employee productive. We've all been in the pre-pandemic position of joining a new organisation where access to all of the equipment, information and applications you need to do your job just isn't quite all there on day one. In a physical office scenario, we could often find ways around this. We'd print documents for people to read, we'd borrow equipment, we'd do face-to-face training and coaching in meeting rooms. We'd get by but at a cost which was rarely measured as lost productivity. In lockdown, unless we were particularly well prepared (and few of us were), productive time was simply lost.

All of the processes that we take for granted; onboarding, offboarding leavers, granting access to systems and applications, resetting passwords and changing roles are big enablers of operational excellence and efficiency. When these processes work well, the business works well, especially when every workload, task and business function is accomplished digitally.

On the customer side, robust management of your digital identities not only enables you to know your customers better but also gets you to the market faster and allows you to scale rapidly. One of the winners from the pandemic is online shopping. Ikea, traditionally a maze-like shopping experience in their cavernous stores, reported a 45% increase in online sales for the 12 months to August 2020. This type of growth requires large scale increases in capacity for e-commerce workloads but more importantly, a digital identity infrastructure that can scale with it and allow for complete self-management of a customer identity whilst preserving security and privacy.

Those with good, identity rich, e-commerce channels that were able to scale quickly in the pandemic have survived. Those without have generally been less fortunate. These are also sticky changes. McKinsey suggests[2] that shifts to online channels, especially where the experience has been positive, will endure.

2 https://www.mckinsey.com/industries/consumer-packaged-goods/our-insights/how-consumer-goods-companies-can-prepare-for-the-next-normal#

2 Identity is a transformation enabler

Business confidence and investment intentions[3] have been steadily growing since reaching an all time low in early 2020. PwC's 24th CEO survey[4] finds that 81% of New Zealand business leaders are planning to increase long-term investment in digital transformation following the pandemic.

These indicators suggest that New Zealand will continue the large programmes of digital transformation that we have seen in both public and private sectors since 2014 but which suffered some pandemic related delays and interruptions.

For those embarking on digital transformation, digital identity is a key enabler. Internally, transformation requires significant changes in operating models and practices. This is underpinned by changes in who does what, with what information and where it is done, as processes are created and adapted to embrace digital developments. There are massive advantages for those who already have a solid understanding of their digital identity. The required structural and operational changes are far easier to implement when you can assign identities to new roles and asset groups. Consequently, this provides a seamless transition to new entitlements, functions and business systems

Typically, digital transformation can be made possible by a large change in single or multiple digital systems which helps reshape what the business does and how it does it. A sound identity management structure and system makes it far easier to integrate these systems whilst a robust understanding of roles and access requirements protects new information services.

Many transformations involve a move to cloud technologies and adoption of large-scale Software as a Service (SaaS) platforms. These implementations are also much more straightforward when you understand and control your digital identities well. By setting up a 'system of trust' between cloud identity providers, users will have a better experience through simplified single-sign-on to a range of new cloud services.

3 https://www.anz.co.nz/about-us/economic-markets-research/business-outlook/
4 https://www.pwc.co.nz/insights-and-publications/ceo-survey/reinventing-new-zealand.html

3 Identity is the foundation of securing your critical assets

Confidentiality is one of the three core tenets of information security and we consider privacy a basic human right. But how do we reconcile this with the fact that our information is now more widely distributed, stored and replicated than ever before

When lockdowns began to happen as the pandemic took hold in early 2020, Zoom, a video conferencing platform saw 200 million user registrations in March alone, from 10 million just three months earlier. In April 2020, hackers breached half a million Zoom accounts and either sold these or gave them away freely on the dark web allowing overt or covert access to private meetings.

What is common in almost all data breaches and cyber attacks is that our human desire to innovate and move forward always outpaces our desire to control, check and test. In a rush to get to market, outpace competitors and often to satisfy stakeholders or investors, applications and platforms will be released with insufficient testing or thinking about and designing for threat and risk.

Identity and access has always been an imperative capability for managing threat and risk, and the pandemic and ransomware events has only increased this threat as organisations have rushed to deploy a remote workforce and service more customers online.

The fundamentals of access control are simple; for each piece of information, define the rules for who can access that information, then every time that information is accessed, ask the identity to prove who it says it is (authenticate) and check if the identity matches the rules (authorise). The first principle is that you are denied access unless it has been clearly permitted. The second principle is that you are only afforded the access and privileges that you need to perform your required function or role; no more, no less.

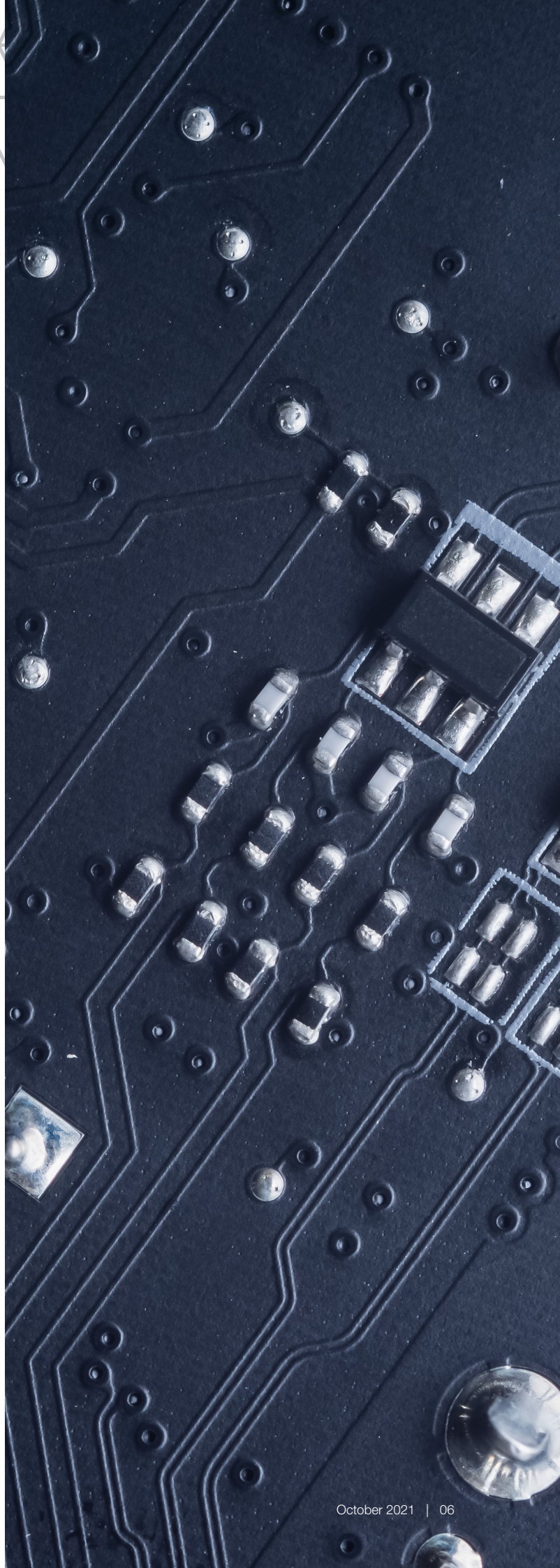
At the beginning of this process is the presentation of identity. This is who I am (or claim to be). Everything else is predicated on this claim of identity. Even when we don't expressly type in a username, systems still require a claim of identity. For example, when you access a website that doesn't require you to authenticate, the system in the background is still processing a claim for an anonymous identity and checking what that anonymous identity is entitled to access.

We can have different identity 'strengths' based on how much confidence we have in the identity claim. An identity presented with a password is much weaker than an identity presented with a fingerprint or biometric. Using these strengths we can control access to high value information or transactions such as banking or healthcare where we must be really sure of who is requesting it.

This combination of identity, identity strength and access rules is fundamentally the core of how information is protected from anyone who shouldn't have access to it. But this apparent simplicity hides a high degree of management complexity.

The management of identity and access rules can quickly get out of hand. Employees and customers come and go, roles change, new information is created all the time and rules can change as context changes.

The only way to have real confidence about 'who has access to what' is to use automation to manage the identity lifecycle (onboarding, offboarding, role changes, etc.) and to monitor access to information and resources. This level of maturity is foundational for achieving Zero Trust architectures aimed at reducing the impact of ransomware events. Then you can use differing identity strengths based on just how important you consider your information (and your users confidentiality and privacy) to be.



4 Identity fosters innovation and confidence

Our latest research shows 91% of NZ CEO's say that they are rethinking their organisations tolerance for risk[5].

Good risk management is the great enabler, but for too long risk management has been seen as a necessary evil and a stick in the wheels of progress. With digital risk, controls around identity, access, and security have been subject to under-investment, outdated thinking and a technology focus. Whenever a significant risk is exposed, the costs (time, human and financial) of mitigation to tolerable levels becomes unpalatable and therefore tolerance increases until the balance sheet looks better. This is often taken to the point at which any remaining control is lip service. Previously, the impacts of risk realisation have not been taken seriously but COVID-19 has and is changing this view.

The risks of digital identity are manifold and new risks are emerging all the time. Consider the current race to develop a viable vaccine passport. The prototypes are all digital (with some analogue alternatives). The idea that an individual will need to demonstrate a health indicator, linked to their identity in order to participate in society, and that this indicator will be derived from health records in some digital way introduces a whole new raft of technical, political, social and legal risks.

However, getting a grip on the fundamentals of establishing and managing digital identities in ways that work now and in the future can only be good for reducing these risks. Once a risk is truly (i.e.measurably) reduced to a realistic level of tolerance then confidence, trust and opportunity follow.

Without confidence, innovation can be stifled by overzealous reactions to regulation and compliance. In European banking, online applications for new accounts are subject to a range of legislation and regulations, and the application process is typically designed by the compliance department. Research from Javelin Research[6] shows that only 8% of successful account applications were completed start to finish on a mobile device. These abandonment rates are unsustainable for any online business but to change the user experience requires confidence.

Imagine a position where you regularly test and check that your identities, customer, citizen or employee, really are who they claim to be. You should also regularly test and check that these individuals can only access the resources they are entitled to because you have sound and robust management of your entire digital identity landscape.

5 https://www.pwc.co.nz/insights-and-publications/ceo-survey/reinventing-new-zealand/risk-conversations-must-be-broadened.html
6 https://www.forbes.com/sites/ronshevlin/2019/10/07/why-cant-banks-get-digital-account-opening-right/?sh=2c78c8533bfd

5 Digital identity is the only future identity

In March 2021, the United Nations Conference on Trade and Development (UNCTAD) published a new report COVID-19 and E-Commerce: A Global Review[7] which reflects on the impact of the pandemic on global and regional digital and e-commerce sectors.

In the report they say that 'it seems likely that the accelerated trend towards e-commerce seen during the pandemic will be sustained during recovery'. Whilst there remain global inequalities in access to technology and the internet, there can be no doubt that there is no return to analogue equivalents.

RealMe, the New Zealand Government's digital identity and identity verification service, has grown from less than 100,000 verified identities at the end of 2015 to almost 800,000 verified identities by July 2020.

In Australia, the Government digital identity is already used by more than 1.6 million people.

Both the New Zealand and Australian Governments are embarking on transformation programmes for digital identity that recognise the need to modernise and scale their efforts to be fit for future growth. Last year, the Department of Internal Affairs received an additional $15m in funding to support the digital inclusion action plan focused on key inclusion elements of access, skills, motivation and trust.

The World Bank ID4D initiative states its goal as 'for all people to be able to access services and exercise their rights, enabled by digital identification'. Using the ID4D data, Mckinsey estimates[8] that 3.2 billion people globally have some form of ID and a digital trail.

> "Nowhere is this more apparent than in the adoption of digital identities. The opportunities to consume and receive services, buy products, manage life events and participate in a functioning society have reached a tipping point of value creation where a digital identity is an everyday and essential part of life."
>
> **Craig Maskell, Cyber Partner, PwC New Zealand**

7 https://unctad.org/webflyer/covid-19-and-e-commerce-global-review
8 https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

The future – underpinned by digital identity

As the world re-shapes post-pandemic, digital identity management will become even more fundamental to successful business transformation, efficient business operation, and as a key enabler for any organisation that provides any form of digital service or product. There are significant opportunities and competitive advantages for those that embrace the power and potential of digital identity. Key steps towards effective digital identity management include:

Implement effective digital identity within your organisation to increase workforce productivity and operational efficiency

Ensure robust management of your customer's digital identities to enable faster go-to-market and the ability to scale rapidly

Use sound digital identity practice to underpin digital transformation of your digital services

Be confident in your confidentiality, privacy and information security by ensuring the fundamentals of access control are in place

Establish a digital position where you have confidence in identities, so that you can truly foster innovation

How we can help

PwC's digital identity practice focuses on strategic outcomes for clients using a business-led and customer-centric approach. Digital identity governance is a fundamental challenge for many businesses, so PwC's digital identity specialists apply their expertise to help clients take control of their identity and access landscape. The team works closely with clients to improve productivity and reduce operational costs and risk, while enabling the workforce to access the right services and information securely.

Contact us

Craig Maskell
Cyber Partner
+64 21 915 380
craig.a.maskell@pwc.com

Sean James
Cyber Director
+64 22 020 0761
sean.c.james@pwc.com

pwc

pwc.co.nz

NZDT-128005786