DIGITAL IDENTITY.NZ

DIGITAL IDENTITY IN AOTEAROA

Identity and Trust in an Increasingly Digital New Zealand

An analysis of the potential impact and opportunities of Digital Identity for Aotearoa New Zealand's economy and society.

digitalnation.nz


2Shakes
ABCorp
Secure since 1795
Access Advisors
ĀHAU I AM
AIR NEW ZEALAND
aws
AML HUB
ANZ
Authsignal
bnz
Bright Partners
GOV.UK
CallaghanInnovation
New Zealand's Innovation Agency
CENTRIX
Credit Bureau of New Zealand
CORE EDUCATION
Tātai Aho Rau
cumulo9
Business certainty, delivered.
DASSET
DATA3
DATACOM
DIF
Te Tari Taiwhenua
Internal Affairs
DLA PIPER
EY Law
FORGEROCK
franklyAi
NO VOICE LEFT BEHIND
Google
Hudson Gavin Martin
Tech, Media & IP
IndigiShare
infolog
Inland Revenue
Te Tari Taake
internetnz
JNCTN
kantara
INITIATIVE
MATTR
Meta
Microsoft
middleware group
MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI
MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA
MinterEllison RuddWatts.
NEC
NEW ZEALAND
TRADE & ENTERPRISE
Te Taurapa Tūhono
NEW ZEALAND
FOREIGN AFFAIRS & TRADE
OCR Labs
PACIFIC
KIDS' LEARNING
paymentsnz
PIM
Personal Information Management Ltd
PLATFORM
Quid Est Veritas
RealAML
Realyou
SafeApp
Simpson Grierson

About Digital Identity New Zealand

Digital Identity New Zealand (DINZ) is a not for profit, membership funded association and a member of the New Zealand Tech Alliance. DINZ is an inclusive organisation bringing together members with a shared passion for the opportunities that digital identity can offer.

It supports a sustainable, inclusive and trustworthy digital future for all New Zealanders through its vision - that every New Zealander can easily use their digital identity. Its mission is to empower a unified, trusted and inclusive digital identity ecosystem for Aotearoa New Zealand that enhances kāwanatanga (honourable governance), rangatiratanga (self-determination and agency) and ōritetanga (equity and partnerships).

DINZ is the voice of the digital identity sector in New Zealand, supporting the growth of the sector.

Member of the: TECH ALLIANCE

Acknowledgments

Digital Identity New Zealand (DINZ) would like to acknowledge the following people and organisations instrumental in bringing this project to fruition:

Our members for their ongoing support and the project sponsors in particular - InternetNZ, AWS, SSS-IT, Datacom and PaymentsNZ.

The Research Sub-Committee of the DINZ Executive Council for wireframing the question sets - Angela Gill (Payments NZ), Ben Dakers (Datacom), Russell Craig (Microsoft) led by Colin Wallis (DINZ Executive Director).

Vica (Viktoria) Papp data scientist at ImmigrationNZ for her review and advice as well as the generational analysis and visualisation done in her own volunteer time.

Ken Aitcheson from New Zealand Trade and Enterprise (NZTE) for his contribution to the export opportunity section.

The Tech Alliance editorial team including Laura Chamberlain, Graeme Muller, Andrea Molloy and the principal writer, Colin Wallis, DINZ's Executive Director.

Lastly, but most critical to the success of this project, the many respondents who gave their time to share their views with Yabble's researchers to enable the capture of the raw data which forms the basis for this report.

Thank you to our Project Partners

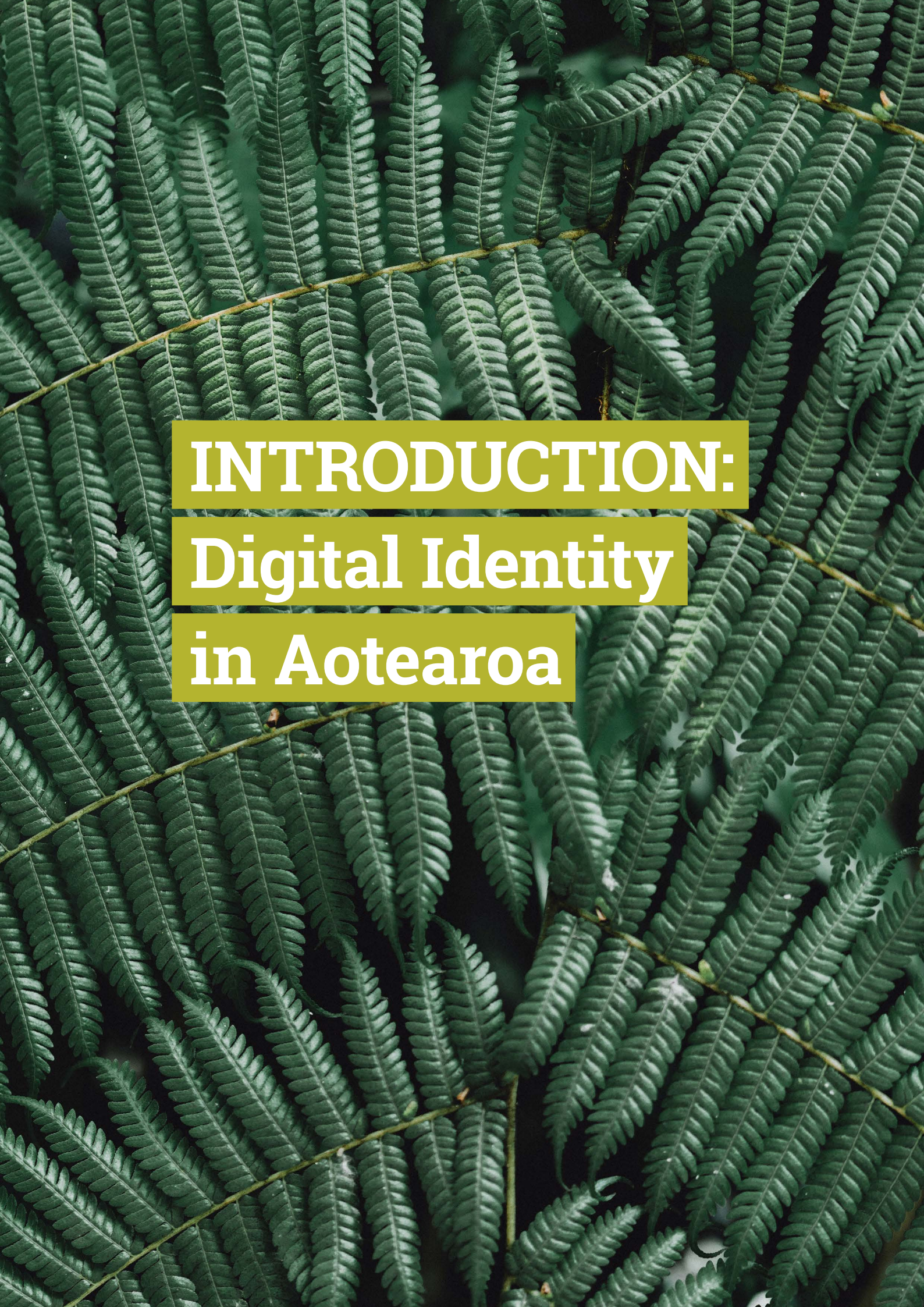
Project Partners

Research Partners

Contents

FIGURES

TABLES



INTRODUCTION: Digital Identity in Aotearoa

FOREWORD:

InternetNZ

InternetNZ is delighted to be the Platinum Sponsor of this Digital Identity New Zealand report, showcasing key themes of building trust and hearing from communities. Nearly every week, the news media will highlight questions of online trust as a force in society, and trust is deeply interwoven with identity.

InternetNZ has its own distinctive role in digital identity as the home and guardian of the .nz domain name system. A domain name gives an identity to a person, business, or computer system that others can remember and rely on. Every time we send an email or visit a website, we rely on domain names to connect us with the right computer systems and the right people. Most people take this for granted, but as the operator of the .nz domain name system, part of InternetNZ's role is to ensure the system works well and upholds the trust people place in it.

This report gathers and shares people's perspectives on digital identity in Aotearoa. While the focus is on business and technology perspectives, there is a clear message about the crucial role of building trust to enable beneficial innovation. People who have doubts about a system will not trust it, and will not use it.

InternetNZ works for an internet that benefits all of Aotearoa. Understanding and upholding the drivers of trust across diverse communities is crucial in order for us to succeed. Progress towards digital equity requires not only delivering connections and technology that people can afford, but working with people in ways they can trust to empower their choices about getting online. Progress towards a more welcoming and beneficial Internet requires better rules and institutions to address behaviours that hurt people and undermine trust.

We have been pleased to support work by Tohatoha, Figure.NZ, 20/20 Trust and Digital Futures Aotearoa who see the value in empowering communities and building trust.

We are encouraged to see the report highlight and embrace Māori perspectives. Identity is central to Te Ao Māori and whakapapa, and connects Māori to who they are, where they come from, and how they relate to others. The history of Government actions and approaches to technology may suggest work to do in this area. This report helps to show some directions for that work to continue.

This is both a challenging and promising time for work on trust and identity in Aotearoa. We were pleased to see the trust pillar of mahi tika highlighted as one of three in the Government's new Digital Strategy, as well as the focus on trust in the Digital Identity Trust Framework legislation. These moves hold out the promise of approaching technology in ways that engage with people's concerns and needs, serve our diverse communities, and build trust. There is work to do, and this report helps show the way to do it.

Vivien Maidaborn
Tumu Whakarae | Chief Executive, InternetNZ

FOREWORD:

Digital Identity New Zealand

Research is fundamental to the mahi or work of Digital Identity New Zealand (DINZ).

On behalf of our members we continue to curate, publish and share useful information about identity and trust for the betterment of all people of Aotearoa.

Since its establishment, aside from the pandemic's disruptions in 2021, the DINZ community has undertaken annual attitudinal research. This research aims to detect trends and shifts in people's views on personal information, how they feel about sharing it to gain the benefits of digital access to services and entitlements, their online behaviour to guard against fraud and their challenges. Underlying these trends and viewpoints is trust. Without ubiquitous trust, the digital economy will remain throttled. As a result, its potential will not be fully realised as segments of society choose not to, or cannot participate.

The introduction of the Digital Identity Services Trust Framework Bill into Parliament in September 2021 heralded a fundamental change in the trajectory of digital identity and trust in Aotearoa New Zealand. For the first time, the domain would be subject to opt-in regulation to codify digital identity. With public or private sector service providers demonstrating their digital services meet recognised capabilities in information security, data protection and privacy for the safety and security of people accessing digital services. The Consumer Data Right, still in development, is additional legislation that will enforce compliance with good practice. In tandem, the legislation aims to differentiate services conforming to the rules and standards enforced by this legislation from those services that don't.

Digital Identity NZ has compiled this research to provide a context for the emerging legislative environment and the challenges being faced by the stakeholders. This report also includes recommendations for the industry to grow and thrive. The challenges to the successful emergence of a vibrant digital identity sector are encompassed by a broader set of challenges that face the New Zealand tech sector. This includes skills shortages, a small domestic market and the successful integration with the global market.

Paul Platen
Chair, Digital Identity New Zealand

Executive Summary

Digital Identity underpins nearly all online transactions and most of our digital experience.

Digital Identity allows people and organisations to use their personal information, including date of birth, income and other proof attributes to access services. Essentially, Digital Identity is a shorthand for the processes used to confirm identification, authentication and authorisation.

Digital Identity is derived from the process of identification in the physical world. Earlier in civilisation this was done at a local level, where the head of the village would vouch for your identity. However in the digital world, you need to prove who you claim to be because you cannot be seen physically in person.

In the modern world, the most commonly known authenticator has typically been a username and password combination. This is changing rapidly with emerging passwordless approaches to authentication. Today, continual improvements in our online experience, means we are often not even aware an identification process is even occurring. As with most components of digital transformation, the online world is in a constant cycle of innovation. Emerging and existing technologies, coupled with better processes and new policy all contribute to reducing risks, improving security, data protection and privacy.

The New Zealand Government's Digital Identity Services Trust Framework (DISTF) is a good example of following other typically comparable countries. The DISTF establishes rules to protect the privacy and security of people's information when it is shared within the trusted environment.

Aotearoa's high level of digital literacy means that most of us are experiencing the digital world daily. However, it's not universal, with significant portions of society excluded from participating for a range of reasons. This follows a similar trend seen in comparable nations around the globe, despite differences in culture, legal basis and values.

Additionally, Aotearoa's context includes an increasing focus on understanding and responding to tikanga, Māori customary practices or behaviours. It is this combination of factors which lies at the foundation of Digital Identity New Zealand's (DINZ) vision - that every New Zealander can easily use their digital identity. This is delivered in its mission - to empower a unified, trusted and inclusive digital identity ecosystem for Aotearoa New Zealand that enhances kāwanatanga (honourable governance), rangatiratanga (self-determination and agency) and ōritetanga (equity and partnerships).

To enable DINZ to achieve these goals, it undertakes annual research to determine Aotearoa's trends and experiences of digital identity. Our research results are used by both the private and public sector, to help inform policy and strategy.

Consumer Attitudinal Research Highlights

Similar to previous years, there is more desire to have control over one's personal data. There has been some progress towards greater understanding of the importance of data protection. This year's results were consistent with 2020, aside from some areas where seniors and the disabled are less likely to view online data as personal information.

Opening accounts for digital services and having to remember usernames and passwords is still causing significant friction for consumers. This suggests the need for a common ecosystem-wide legislative, legal contract and architecture to allow for coordinated, consented and privacy-centric identity attribute exchange.

The continued lack of confidence in managing personal information alongside the statistics that six in ten are unaware of how to protect their rights and six in ten have experienced misuse of their personal data, mainly through credit card

fraud, reinforce the need to raise awareness and education amongst the general population.

Three quarters of respondents were still wary of the transparency amongst organisations using their data and a similar proportion were unhappy about the idea of organisations sharing/selling their data. As shown next, while it's encouraging that most businesses who undertake digital identity processes intend to become accredited under the upcoming Digital Identity Services Trust Framework (DISTF) Act, its multi modal and multi channel nature means this is only the start of the process.

Business and Organisation Research Highlights

The recent introduction of the DISTF Bill signalled the Government's commitment to regulating the emerging ecosystem of digital identity service providers. This includes the private and public sectors, both domestic and global. It also reflects the trajectory of other common law jurisdictions that Aotearoa typically compares itself to.

For the first time, DINZ conducted business facing attitudinal research in parallel to its established consumer research. The aim was to better understand the attitudes of this critical component of digital transformation. It included organisations offering consumer facing internet based services where nearly all operate digital identification and/or digital verification services directly or via a third party.

Encouragingly, the research showed business has a good understanding of where to find applicable legislation and awareness of upcoming legislation.

However, the results were less encouraging regarding the skills and tools to protect their customers' personal information. Only one third of businesses feel fully equipped to protect their customer's personal data, while one quarter find this easy to do. Similar to the public/consumer research, the need for more education of staff was identified. However, in the case of businesses this was lower, at 40 percent, versus 60 percent for consumers. These results support the consumer research conclusion that there is a trust problem.

From the service providers perspective the level of capability is not high enough. Eight out of ten organisations surveyed support the introduction of a Consumer Data Right (CDR) and DISTF legislation and six out of ten intend to be certified. This shows the industry's acceptance of a regulatory regime as a key motivator to lift trust and capability.

Where to from here?

There are significant economic benefits to be gained from reducing friction in digital identification. How can we harness these benefits and export trust? How can we leverage our strong international reputation for honesty and lack of corruption to position ourselves as trusted?

The following sections review the research results in further detail and preliminary recommendations are provided for further discussion.

The recommendations (summarised on the next page and provided in detail from page 34) can be divided into four key themes:

1. Build trust

2. Increase education and understanding

3. Drive confidence and engagement

4. Develop the Digital Identity sector

Summary Recommendations

This research highlights that the issues holding back more rapid uptake of digital identity and hence the growth of the digital economy have remained consistent for the past four years. These issues stem from a lack of trust, understanding and confidence. Consequently, Digital Identity New Zealand provides the following recommendations, distilled from the research, to support the collaborative improvement of the Aotearoa digital identity ecosystem.

The full recommendations can be found on page 34.

THEME ONE - Build trust

1.1 The Government must encourage businesses to pursue multiple avenues to demonstrate trusted services for the public.

1.2 Businesses must actively participate in frameworks available to create and demonstrate trust.

1.3 Businesses and Government agencies must increase their investment in security measures that protect customer information, and in cybersecurity in general.

THEME TWO - Increase education and understanding

2.1 The Government should help develop best practice guides for service providers to help them educate users visiting their sites.

2.2 Businesses must improve the provision of security information and education for users on their web pages.

2.3 Businesses and Government agencies must increase investment in the education of their own staff with respect to protecting their customers' data.

THEME THREE - Drive confidence and engagement

3.1 The Government should ensure that identity services cater for all sectors of society and that all sectors of society have the skills and confidence to engage with these services.

3.2 Businesses must develop their online presence in ways that make it easier for people to understand how to protect their personal information in culturally appropriate ways.

3.3 Businesses and Government agencies should be encouraged to use plain language summaries of their key messages such as privacy statements and user agreements.

THEME FOUR - Develop the Digital Identity sector

4.1 The Government should encourage service providers to also look toward non legislative best practices regarding personal information protection, processing, storage and deletion.

4.2 Businesses should appoint a data security lead, or a role that oversees data security and privacy.

4.3 Businesses and Government should collaborate with Digital Identity New Zealand to create a national culture of best practice for protecting people's information online.

Key Highlights
Consumers

90% of New Zealanders believe it is not easy to protect their information online.

90% of New Zealanders find the idea of being more in control of their digital identity appealing.

78% of New Zealanders are concerned about the protection of their identity and the use of personal data by organisations.

70% of New Zealanders place some onus on the organisation holding their data, but there is some sense of shared responsibility.

60% of New Zealanders don't feel they know how to protect their information.

60% of New Zealanders are satisfied with the process of registering personal details with Government agencies in response to the COVID-19 pandemic.

60% of New Zealanders have experienced some form of misuse, with credit card theft being most common.

50% of New Zealanders know their rights regarding the protection of personal data.

50% of New Zealanders have adapted their online behaviour due to concerns around data privacy.

50% of New Zealanders have some issue with registering new accounts online, although there has been a significant increase in satisfaction since 2020.

Key Highlights
Businesses

80% of businesses know where to find relevant legislation for their digital security obligations.

33% of businesses feel equipped to protect their customer's personal data, while just 25% find this easy to do.

40% of businesses undertake the most common security measure - erasure of data - but overall security measures are underutilised by businesses.

40% of businesses believe better education of their workforce and increasing awareness/understanding of threats would help further protect and manage personal identity related data.

33% of businesses believe the pandemic has impacted the way they manage their customer's personal data.

Approx. **50%** of businesses have not sought external advice on cybersecurity and data protection.

80% of businesses believe that the Digital Identity Services Trust Framework (DISTF) and the proposed Consumer Data Right (CDR) legislation is necessary in New Zealand.

60% of businesses engaged in digital identity processes, intend to become accredited under the DISTF Act.

PART ONE: Exploring the Digital Identity Landscape

Introduction

Trust lies at the heart of human relationships. While the notion of trust has been with us since the beginning of humanity, it is rooted in the physical world, where people can be close to each other and understand their heritage. Over time, sources of authority were able to vouch for an individual's integrity. In the past, just as today, this extends to commerce and entitlements. In a digital world where this physical closeness doesn't exist, other methods are required to gain confidence and assurance in someone's identity and data. This includes overall security of the system and the personal data it processes to ensure the parties are acting in good faith. Without digital trust, the digital economy falters and ultimately cannot function.

As the digital age evolves, identification is increasingly undertaken remotely and by digital means. The digital representation of an entity (a person, organisation or a device) has become essential for cybersecurity and data protection. With its beginnings in enterprise, digital identification and verification is now mainstream in nearly all digital transactions. Almost every entity that transacts or engages online, interacts with digital identity.

Digital Identity: An attribute or set of attributes that uniquely describe a subject within a given context.

A global ecosystem has emerged to support this innovation. This includes recompiling existing processes and technology applied to the domain of digital identity, for example decentralisation and cryptography. Plus, emerging new technologies, for example biometrics, machine learning (ML) and artificial intelligence (AI). As a result, the global digital identity landscape is fragmented with sectors at different stages of development and tackling the domain from different baselines, influenced by their own culture and available resources.

What is Digital Identity?

Digital identity is derived from the process of identification in the physical world. Earlier in civilisation this was done at the village level, where the head of the village would vouch for knowing you and your family and that you resided in the village. You transacted by simply appearing at the place where the transaction took place. However in the digital world, you need to prove who you claim to be because you cannot be seen physically in person. This having been proven, two things typically occur. A unique record is created which is represented by a number or a name in a database. This is often referred to as a unique identifier which enables an individual to confirm their identity, without having to repeat the initial process. This process is called Authentication. The most commonly known authenticator has typically been a username and password combination. Typing a username and password to confirm 'it's me again' provides the other party with confidence and assurance of an individual's authority to access particular resources.

Essentially, Digital identity is a shorthand for this process to confirm your identification, authentication and authorisation that the process has been carried out.

Definitions of digital identity vary across jurisdictions and industry sectors. For example, locally, digital.govt.nz uses the Collins dictionary definition for identification as "the act of identifying or the state of being identified."[1]

The United States of America Department of Commerce defines digital identity as an attribute or set of attributes that uniquely describe a subject within a given context.[2]

Why is it important?

Digital identity underpins the majority of our digital transactions and is the foundation for digital transformation. From banking, loyalty programmes to purchasing products and services, third parties require a level of confidence in digital identity relative to the value of the transaction and risk of fraud. Unless mechanisms assure them that an individual is in control, they will not authorise access.

100% adoption of digital ID coverage could unlock economic value equivalent to 3 to 13 percent of GDP in 2030

Most of us want to go online and access resources with as little friction as possible. Identity proofing once and repeatedly authenticating enables this critical aspect to become ubiquitous in a majority of transactions, particularly repetitive ones.

The Digital Identification and Authentication Council of Canada has published some easy to read use cases which demonstrate the everyday application of digital identity and why it is important.[3] For example, gaining access to healthcare services, shopping online or navigating government services.

Adopting digital identity more widely, also provides substantial economic benefits. In Digital ID: A key to inclusive growth, McKinsey notes that a 100 percent adoption of digital identity coverage could unlock economic value equivalent to three to 13 percent of GDP in 2030.[4]

While here in Aotearoa, Hon Dr David Clark says international studies have suggested the potential benefit of enabling digital identity in a mature economy is between 0.5 and three percent of GDP – so roughly $1.5 to $9 billion in NZD.[5]

The key challenge is, regardless of the jurisdiction, access to and enablement of digital identity is not equitable. Digital inclusion remains a significant global problem.[6]

Consequently, DINZ's recently established an Inclusive and Equitable Uses of Digital Identity Working Group to help address these concerns in Aotearoa. This working group is supported by civil society representatives and has produced an initial discussion paper identifying some of the existing mahi (work) both in New Zealand and globally regarding inclusivity and ethics in digital identity.[7]

Digital Identity around the world

Globally, digital identity is considered to be a high growth domain. In an update from Juniper Research published in August 2022, the market for digital identity verification checks is forecast to reach $20.8 billion globally in 2027; up from $11.6 billion in 2022.[8]

Many industry observers compare digital identity approaches by country, however it is essentially history, culture and legal basis that influences their trajectory. By viewing through this lens, natural groupings emerge. For example, the typically compared countries steeped in common law - Australia, Canada, New Zealand, the

United States of America (USA) and the United Kingdom (UK) - all have a similar, though not identical trajectory, when compared to the civil law countries typically found in the European Union. Countries with established identity (ID) card schemes also have a similar but not identical trajectory, different to those that don't use ID cards. Comparing developed, developing and underdeveloped countries is another lens but still offers more insightful comparison than simply comparing one country with another.

Common Law countries

The common law countries have broadly all adopted similar approaches. Australia and the UK have both trialled forms of ID cards in the early part of the century which were generally rejected by the people and civil liberties groups. This is a sentiment shared by the other common law countries previously mentioned.

At a similar time, Canada trialled a Public Key Infrastructure technical approach for passports which failed, while the USA's REAL ID Act passed by Congress in 2005 following 9/11 is due to come into force on 3 May 2023. This will be mandatory identification to board a plane and has slowly paved the way for a national ID-esque credential.

During the past seven years, all these countries have moved towards a market ecosystem model through the development of Trust Frameworks and their associated standards, rules and certification of conformance. For example, Australia's Trusted Digital Identity Framework, Canada's Pan-Canadian Trust Framework, New Zealand's Digital Identity Services Trust Framework, the UK's Digital Identity and Attributes Trust Framework. While the USA has no overarching trust framework, it has multiple sector based frameworks. Each jurisdiction is developing legislation to enable regulatory enforcement of their Trust Frameworks.

Civil Law countries

Most European nation states' history and culture is steeped in Civil Law and the population registers that rose from them. The registers were mostly used to develop ID cards for identification and proof of age for transactions in society. The European Union was the first trading bloc to introduce legislation, eIDAS (electronic IDentification Authentication and trust Services) came into force in 2018. It was a response to improve the interoperability amongst the Member States in pursuit of the objectives for the European Single Market. While its level of adoption varies widely, it remains the most advanced and mature digital identity framework. In 2022 it is entering its second revision which focuses on a decentralised architectural approach where citizens would have a mobile device enabled digital wallet to hold identity related digital credentials and attributes. Time will tell if eIDAS2 will result in improved interoperability and higher adoption levels.

Other nation states

Most other nation states (autocratic or democratic) have developed digital identification schemes similarly built upon physical ID card beginnings. This tendency was assisted by the World Bank favouring lending to developing nations for ID card based schemes in preference to non ID card schemes. Regardless of the architectural option, digital identification schemes can be used for purposes other than the wellbeing of people. For example, there is a greater risk of instances where ID Cards can be used inappropriately, breaching privacy and a range of human rights.

Pan-Global initiatives

Global platforms including Apple, Google, Meta and TikTok have digital identification systems to both protect and strengthen their

service offerings that span multiple countries. These may be joined in future by sectors with a ubiquitous global presence such as telcos and financial services. The latter leverages their need for strong identification and authentication to comply with anti-money laundering (AML) legislation. Digital identity cross-jurisdiction Government initiatives have been trialled for the past 15 years and are continually refreshed as one initiative is partly replaced by another. The initiatives aspiring to greater cross recognition and interoperability to reduce friction for trade, have made modest progress so far.

Digital Identity in Aotearoa

In 2007, Aotearoa was amongst the early adopters to launching a public facing service, the forerunner to today's RealMe. Initially, the Government Logon Service was not a digital identification service, but solely an authentication service. Its role was to confirm the identifier and associated password was recognised when logging onto a Government agency service.

After the relocation of the Authentication Programme from the State Services Commission to the Department of Internal Affairs (DIA), the Identity Verification Service was added in December 2009, leveraging passports and other authoritative sources of identity related personal information held by the DIA alongside the NZPost network.[9] This enabled people to have their photos taken that the DIA matched with the passport photo held in its registers. Under the RealMe brand, banks and a handful of other non governmental digital services federated with RealMe to avoid duplicating services. This provided an alternative to applicants registering the same information for multiple services. In parallel, the DIA operated various similar verification services to authorised third parties,

In 2019 the digital identity ecosystem was strengthened with he establishment of Digital Identity New Zealand.

where authorised service providers could submit applicants' claims of identity attributes and have them verified against DIA's registers without the need to federate with RealMe. These back office services assisted the rise of a range of private and public sector digital identity service providers across Aotearoa into an emerging ecosystem. This was reflective of the developments in Australia, Canada, the UK and the USA.

In 2019, the digital identity ecosystem was further strengthened with the establishment of the industry association, Digital Identity New Zealand (DINZ). The drafting of the Digital Identity Services Trust Framework Bill (also reflecting overseas developments) and its introduction to Parliament in September 2021, completed the information security, personal data and privacy wireframe for a digital identity ecosystem to form, flourish and be trusted.

The rate, focus and maturity of the ecosystem's development is significantly dependent on Government funding. After years of underfunding, in 2022, RealMe was awarded Budget funding over four years to improve its service offerings and online customer experience. Meanwhile, funding to support the development of the rules to operate the regulation of the Trust Framework was put on hold until Budget 2023.

While striving for good, robust, safe and privacy respecting digital identification, challenges remain. The need to focus on tikanga is culturally specific to te ao Māori whakapapa and cannot be adopted from comparable countries in the way that much of the digital identity ecosystem has been. This is clearly illustrated by the effect on taonga regarding mana in the storage of facial images and other identifying attributes away from the person (in an on-premise or cloud server). However Aotearoa does share one trend with its counterparts. Distrust of government authority and the conspiracy theories surrounding it attract a significant following and digital identity - indeed everything digital in the views of some - is seen to be complicit in it. It is important to appreciate that 'digital identity for good' and 'digital identity for bad' is largely separated merely by culture, law, the system of government and the ethics and morality of those operating it. From a technology standpoint, the difference between 'good digital identity' and 'bad digital identity' is not necessarily on opposite ends of the continuum.

This is why DINZ's annual attitudinal research is so important. The research baselines help policymakers, industry and the public better understand the trends and changes in attitudes to digital identity, plus the challenges encountered. In the 2022 research, an additional survey of businesses was conducted to determine the level of awareness of impending legislation, obligations regarding personal information which is personally identifiable information under the Privacy Act 2020, and to begin to understand their challenges. Research highlights are featured in the next section.

PART TWO: Digital Identity Attitudes

Understanding our attitudes

Our annual research aims to detect trends and shifts in people's views on personal information, and how they feel about sharing it to gain the benefits of digital access to services and entitlements. It also explores individual's online behaviour to guard against fraud and their challenges.

The introduction of the Digital Identity Services Trust Framework Bill into Parliament in September 2021 heralded a fundamental change in the trajectory of digital identity and trust in Aotearoa. The Consumer Data Right, still in development, is additional legislation that will enforce compliance with good practice. In tandem, the legislation aims to differentiate services conforming to the rules and standards enforced by this legislation from those services that don't.

Digital Identity NZ has compiled this research to provide a context for the emerging legislative environment and the challenges being faced by the stakeholders. This year we have undertaken additional research on business perspectives, particularly those that operate online digital services. Accordingly, the research is presented in two parts - Consumer and Business.

Consumer Survey Demographics

The New Zealand Digital Identity Attitudes Survey has been conducted in 2019, 2020 and 2022 by Yabble Research on behalf of Digital Identity New Zealand. Due to the pandemic, no survey was conducted in 2021.

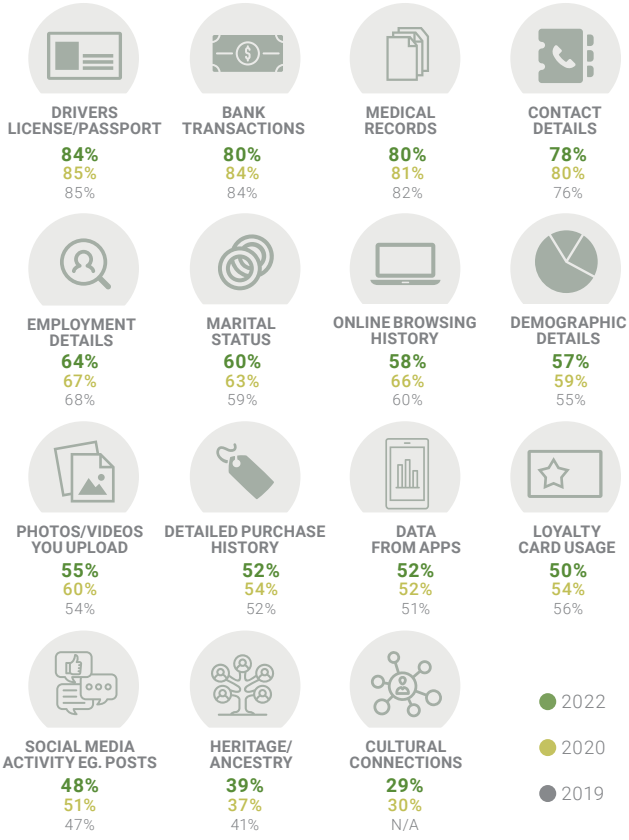
The survey was conducted online with large sample sizes to obtain proportional representation across age, gender, ethnicity and location.

The 2022 survey was completed by 795 people. In 2020 it was completed by 1011 and 2019 by 1092 people. The 2022 target sample size for the general public was smaller than previous years due to the sample split between the general public and business (separate surveys). Please refer to the appendix for the methodology and sample demographics.

Shared responsibilities and Kiwi's key concerns

New Zealanders consider a broad range of information held about them as personal data or information. For example, as detailed in Figure 1, passports, driver's licences, bank transactions, medical records, address details, employment details and more. Fewer consider online data such as browsing history, social media posts or online purchase history as personal information. This is consistent with previous years research, however seniors and the disabled are less likely to view online data as personal information.

Figure 1 - What do New Zealanders consider personal data



Source: New Zealand Digital Identity Attitudes Surveys, 2019, 2020, 2022. Note that 11 respondents explicitly selected 'none of these'.

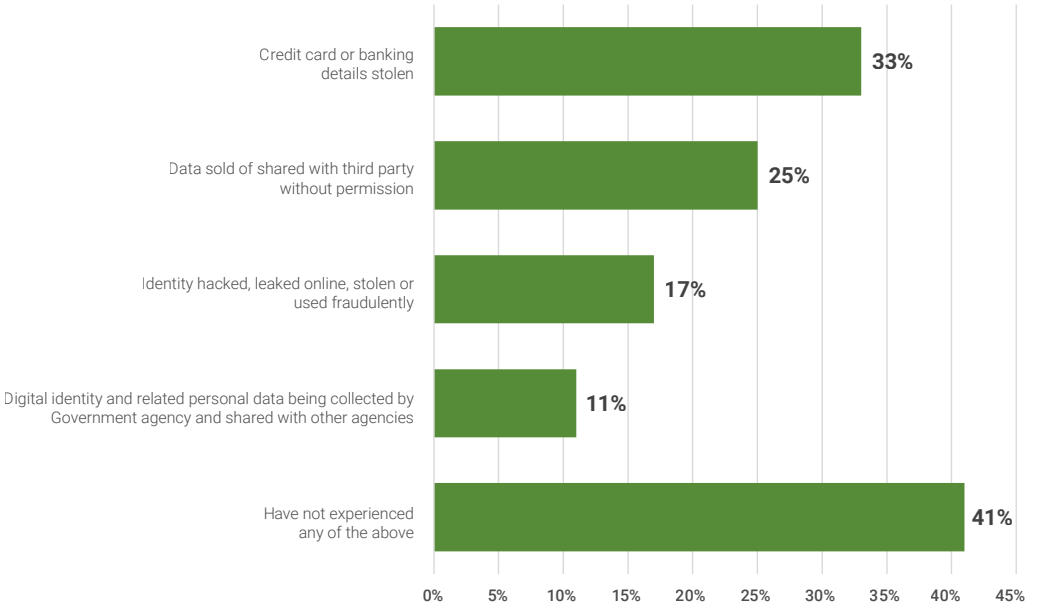


Figure 2 - Personal experience regarding identity and use of personal data

Source: New Zealand Digital Identity Attitudes Survey, 2022. Note some respondents selected multiple answers which accounts for greater than 100%.

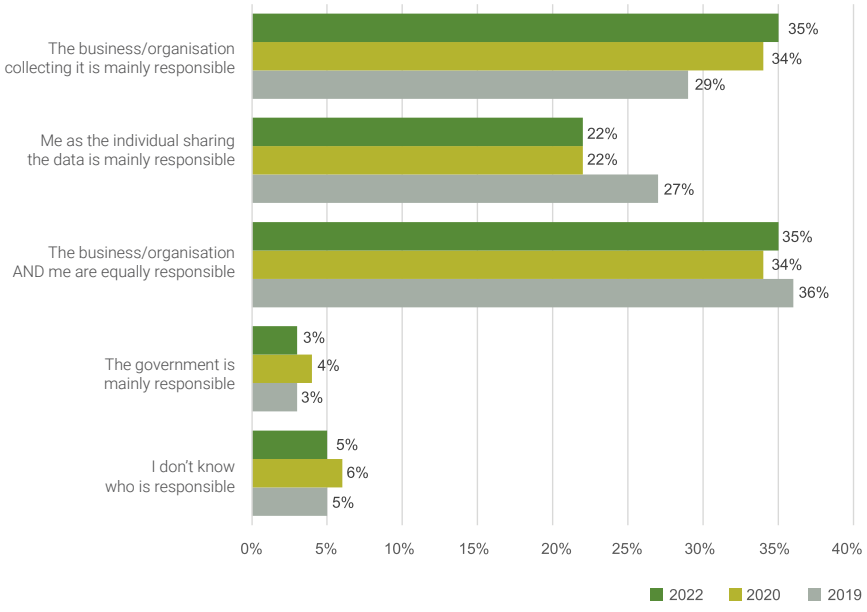
The key trend continues - a high level of concern regarding personal information protection. The survey found that 78 percent of New Zealanders are concerned about the protection of their identity and use of personal data by organisations. In comparison, 2020 survey results recorded three percent less at 75 percent.

As shown in Figure 2, six in ten New Zealanders have experienced some form of misuse, with credit card theft being most common. Naturally, this can increase an individual's concerns regarding data protection.

There is a sense of shared responsibility, with seven in ten New Zealanders placing at least some onus on the organisation holding their data. However, over time the expectations around shared responsibility have been changing with individuals increasingly identifying the business or organisation collecting their data as being responsible for protecting it.

During the past three years, as seen in Figure 3, the expectation that the Government is responsible for protecting citizens data has remained consistent at three percent. However, the proportion of people who consider themselves as mostly responsible for protecting their data has dropped from 27 percent

Figure 3 - Responsibility for protecting personal data and ensuring it is used responsibly



Source: New Zealand Digital Identity Attitudes Surveys, 2019, 2020, 2022.

in 2019 to 22 percent in 2022. Meanwhile, those who see businesses or organisations collecting the data as mostly responsible has risen from 29 percent in 2019 to 35 percent in 2022.

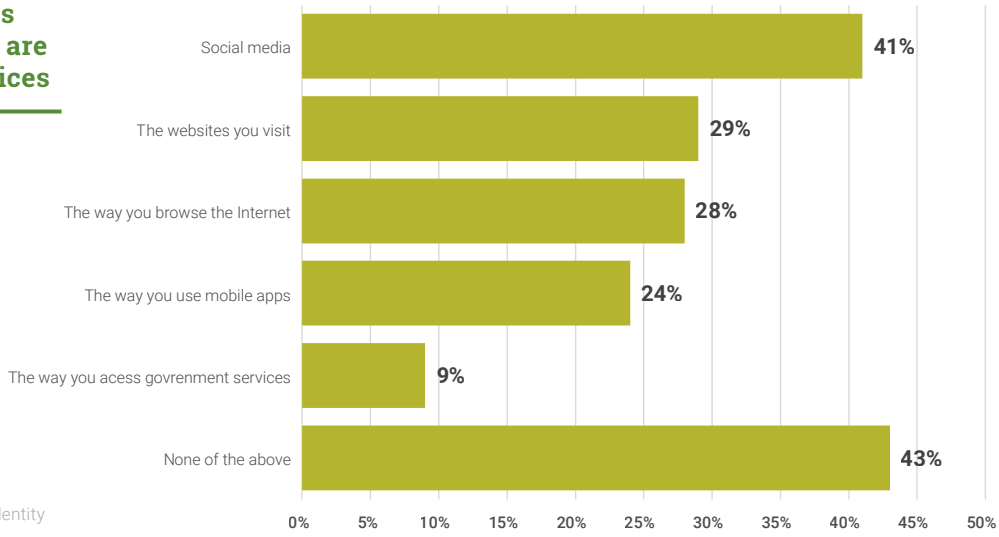
Notably, there was a higher than average representation of Pacific Peoples who indicated they didn't know who was responsible or who thought they may be responsible for protecting their own data.

The survey asked participants if due to their concerns, they had made any changes to the way they use a range of online services. The responses, shown in Figure 4, are consistent with previous years. A significant number of respondents indicated they have been making changes to the way they use online services due to concerns about data and privacy.

However, there was still a large number of people, 43 percent of respondents, who have not made any change to their online behaviour to protect their privacy or data.

Analysing the data deeper, Māori respondents were more likely to have adapted the way they use social media, visit websites, browse online or use mobile apps due to privacy concerns than the national average. Meanwhile, senior respondents were less likely to have adjusted their online behaviour.

Figure 4 - Changes in the way people are using online services



Source: New Zealand Digital Identity Attitudes Survey, 2022.

Do we know how to protect our online data and information?

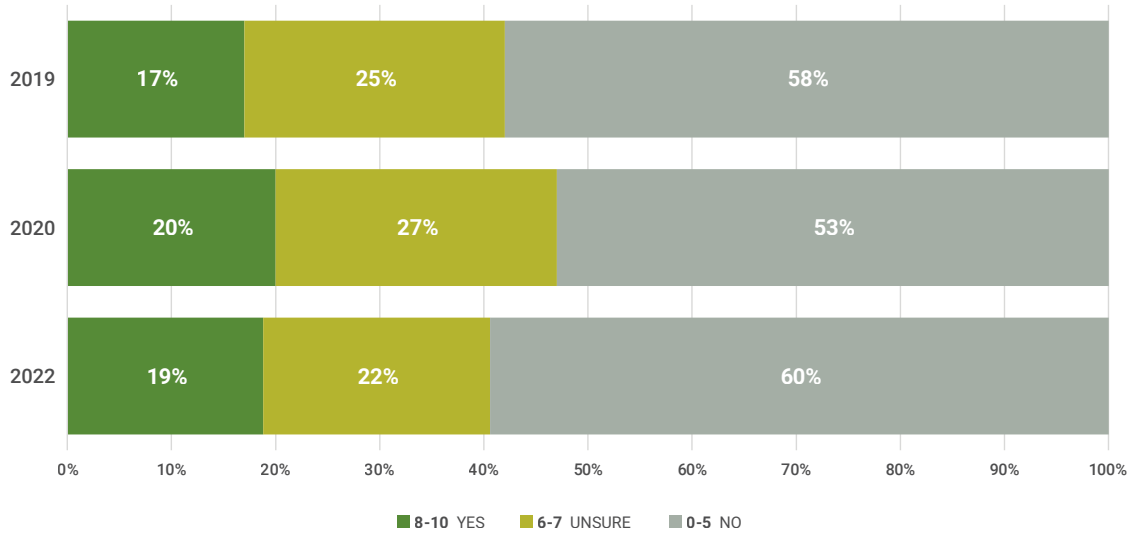
There continues to be a considerable lack of knowledge of how to protect identity and control data use online. Our new research shows, in Figure 5, six in ten New Zealanders don't feel they know how to protect their information. This has increased from 53 percent in 2020.

Not only do most Kiwis not know how to protect their data online, the majority also find it difficult to protect their identity and control the use of their data online. Figure 6 shows that almost nine out of ten people don't find it easy to protect their identity online. This has shown no improvement across the past three annual surveys.

While most find it difficult to protect their identity online, New Zealanders are currently using a range of tactics in an attempt to be more secure. For example, as shown in Figure 7, over half of respondents do not save their credit card details on e-commerce sites and 43 percent use multi-factor authentication where available. However, the number of respondents using tactics to protect their data is generally low.

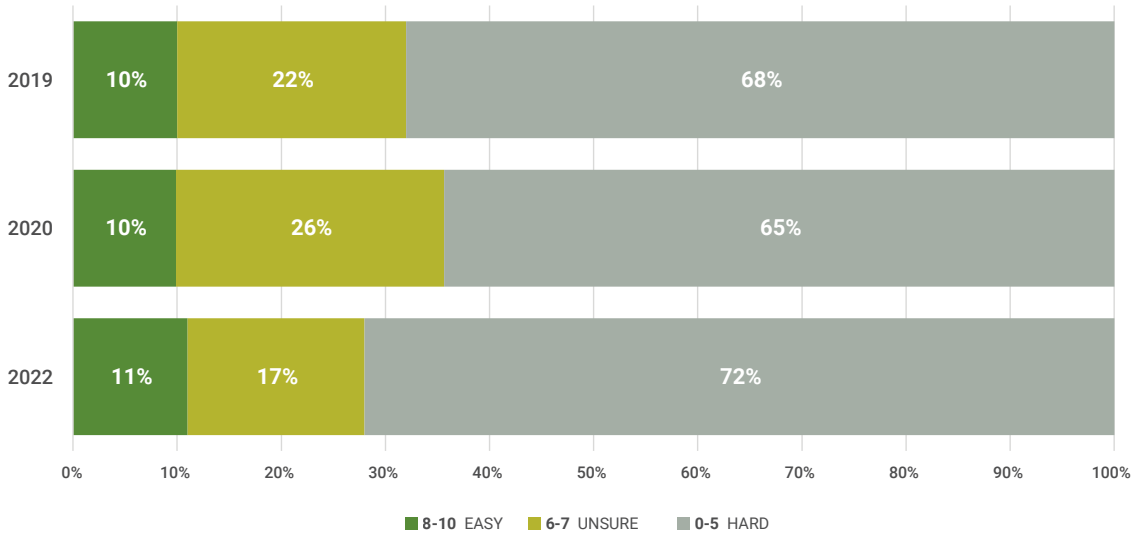
This lack of knowledge, the perceived or real challenges and low levels of engagement in simple methods clearly indicates the importance of information and education. This is essential to help build trust in the digital economy.

Figure 5 - Do you know how to protect your identity and control use of your data online?



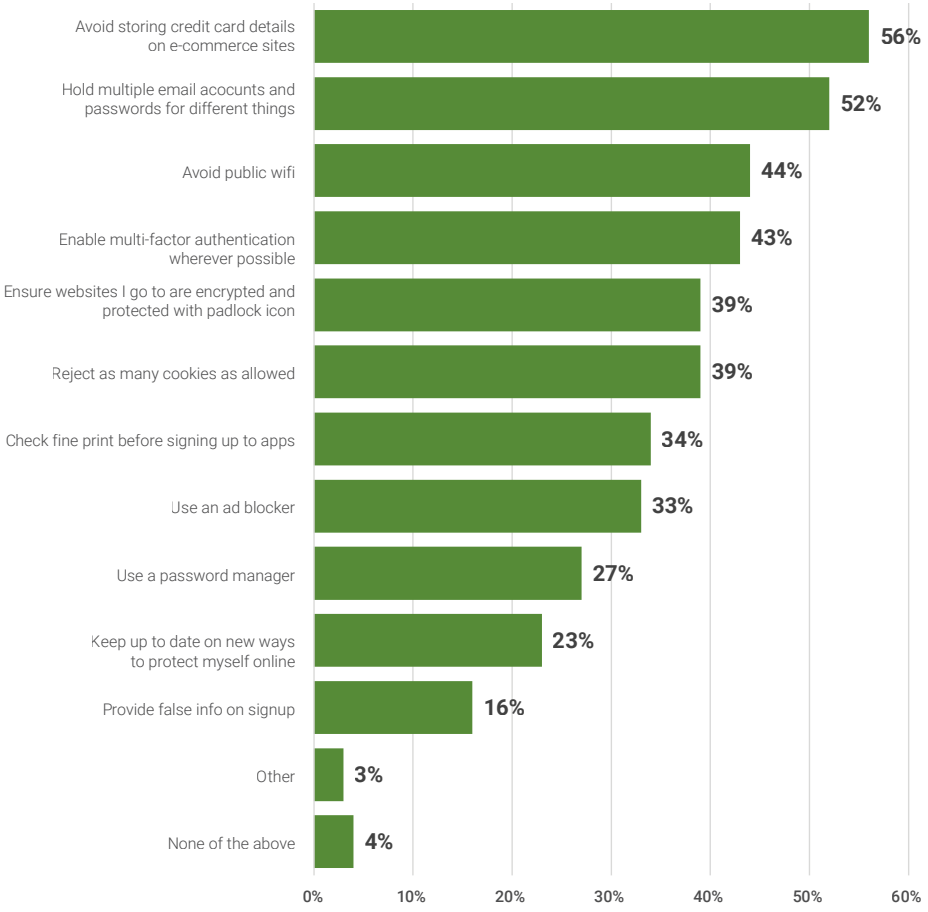
Source: New Zealand Digital Identity Attitudes Surveys, 2019, 2020, 2022.

Figure 6 - How easy is it to protect your identity and control use of your data online?



Source: New Zealand Digital Identity Attitudes Surveys, 2019, 2020, 2022.

Figure 7 - Actions taken to protect digital identity online



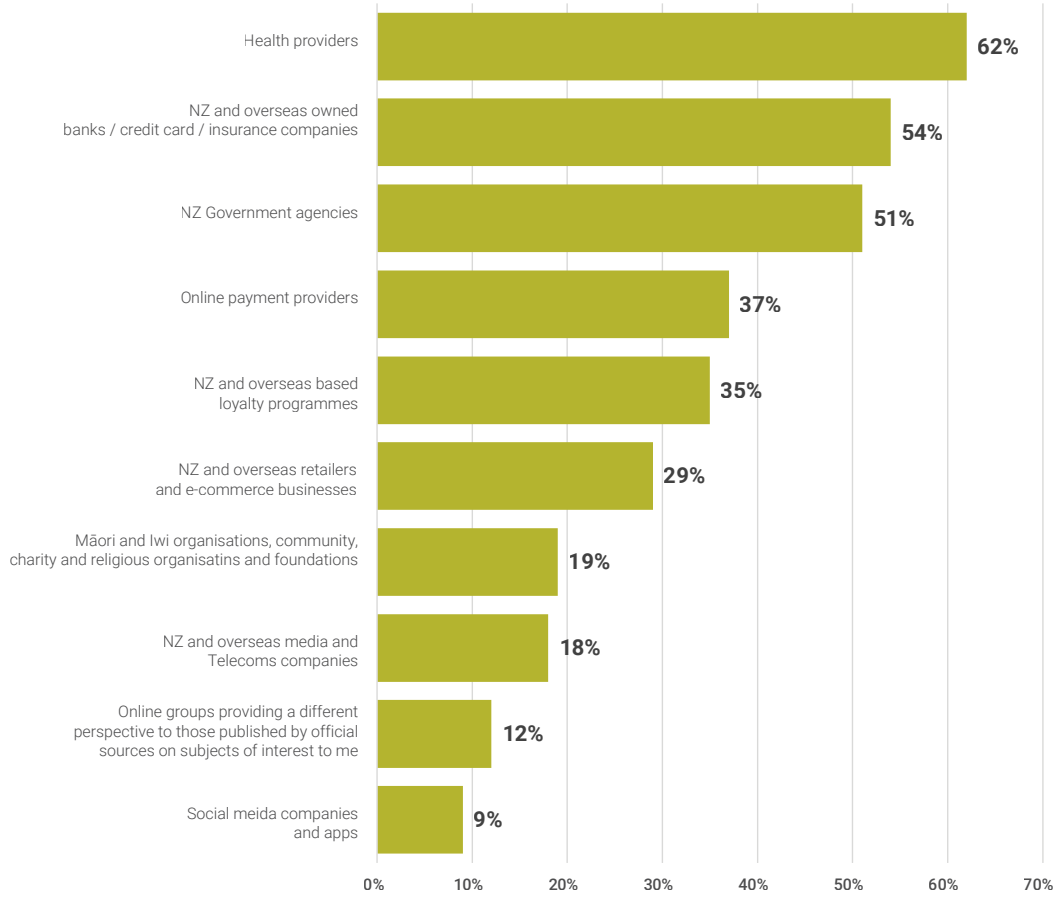
Source: New Zealand Digital Identity Attitudes Survey, 2022.

Who do New Zealanders trust with their data?

According to the 2022 survey respondents, New Zealanders do not trust social media companies to protect their digital identity or use their personal data responsibly with only nine percent indicating trust. At the other end of the spectrum, health providers maintain relatively high levels of trust with 62 percent of respondents trusting them to use their data responsibly.

Financial institutions were the next highest trusted organisations with 54 percent trusting them with their digital identity and responsible use of their data. With digital identity being a critical foundation for managing our money in the digital world, financial institutions have an advantage even over Government agencies that are only trusted by half of the population to manage our data responsibly.

Figure 8 - Extent that organisations are trusted to protect identity and use personal data responsibly



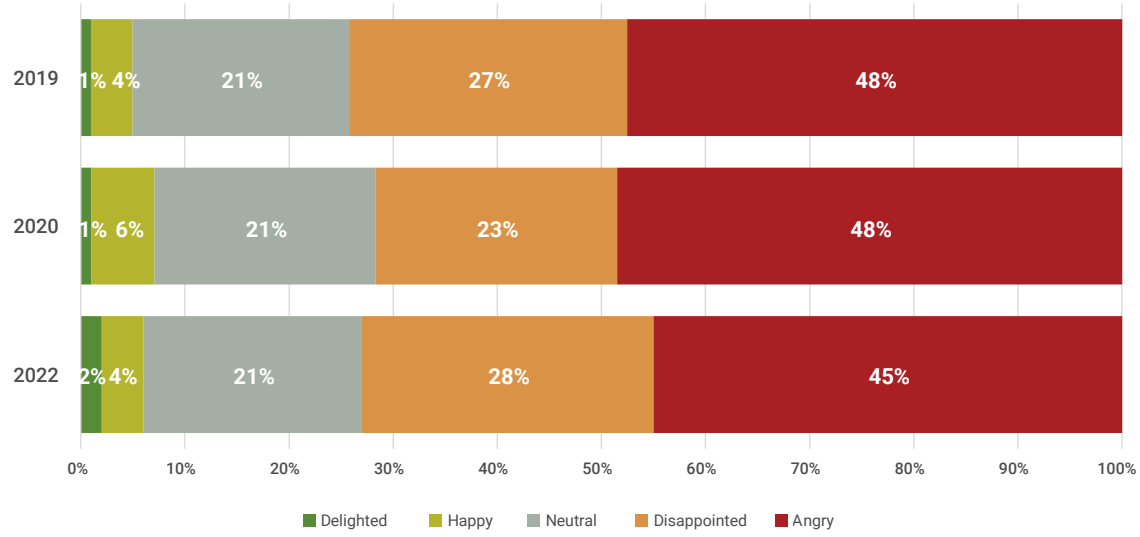
Source: New Zealand Digital Identity Attitudes Survey, 2022.

How do we feel about organisations sharing our data?

Sharing and selling of data elicits high levels of negativity amongst New Zealanders. Since 2019 almost half of all respondents feel angry about organisations sharing or selling their personal data to a third party. In the 2022 survey, 45 percent of respondents indicated that this practice makes them angry, slightly down from 48 percent across 2019 and 2020. A further 28 percent feel disappointed when an organisation shares their data with a third party. Across the three years a fifth of respondents were neutral and very few happy. In 2022, knowing an organisation has shared their data with a third party only made 4 percent of respondents happy and 2 percent delighted.

Almost three quarters (73 percent) expressed feeling upset when they find out an organisation has shared their data with a third party.

Figure 9 - Feelings about organisations that share or sell your data to third parties



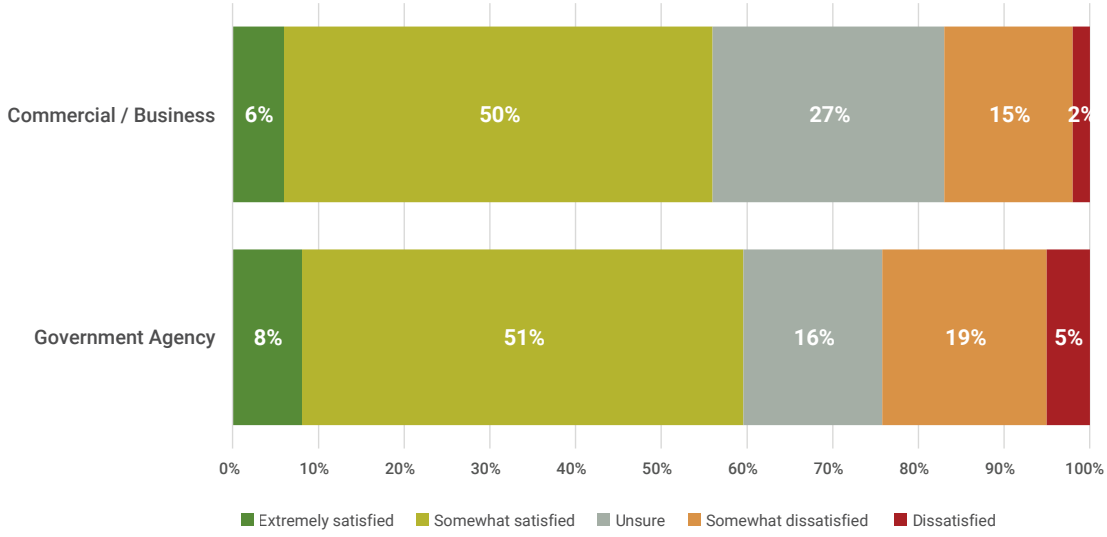
Source: New Zealand Digital Identity Attitudes Surveys, 2019, 2020, 2022.

A satisfying online experience?

There has been an increase in the people that are somewhat satisfied with their online experience since 2020, lifting from 44 percent to 50 percent. Additionally, since 2019 the overall level of combined dissatisfaction has decreased from 22 percent to 17 percent.

As shown in Figure 10, satisfaction with commercial organisations appears to be quite variable with 56 percent expressing some level of satisfaction and 17 percent dissatisfied with their experience creating a new account. Whereas the experience with Government agencies is more polarised with 59 percent satisfied and 24 percent dissatisfied.

Figure 10 - Satisfaction with experience of registering new account



Source: New Zealand Digital Identity Attitudes Survey, 2022.

Do we want more control?

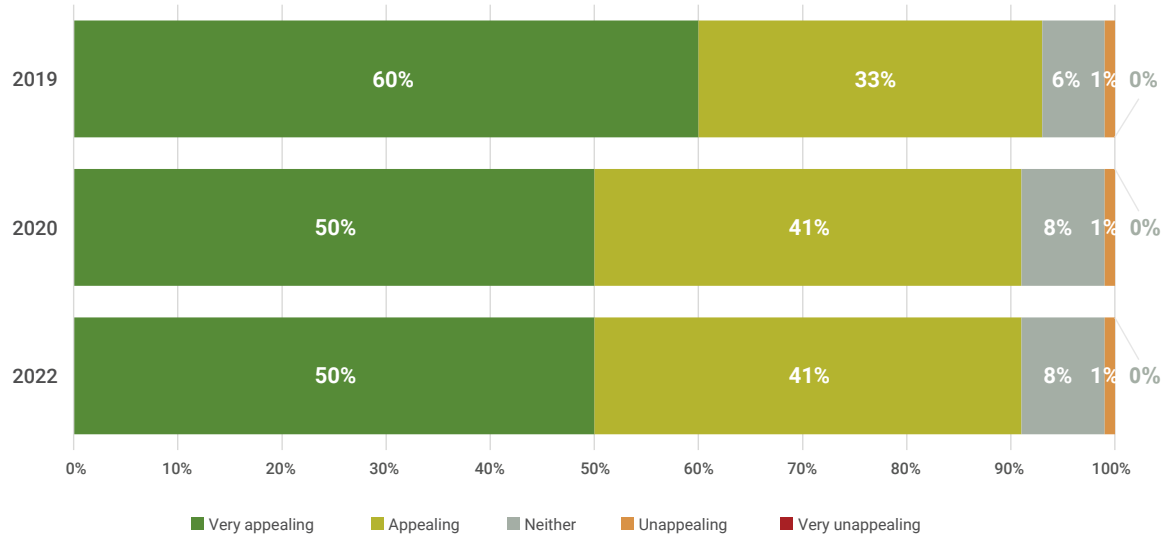
Yes, as shown in Figure 11, nine out of ten New Zealanders find the idea of being more in control of their digital identity appealing. This has been consistent over the years and the message is very clear. Organisations that can provide ways for their customers (or citizens) to have more personal control and ownership over their online identity and personal information will better meet their customer's wishes.

When asked about their views, similar attitudes have been reflected over the years. However, in 2022 we see the emergence of people interested in monetising their digital identity data. Other ideas relating to people's desires for more control of their data are described in Table 1. Table 2 shows examples of the key concerns people have if they were to be given more control over their data and digital identity. These concerns mainly involve a lack of understanding of what it would mean or how to do it. Plus worries that it would take more effort or cost more.

Table 1 - Why we want more control of our data

2022	2020	2019
It would make them feel more secure/more control • "I like the idea of having control of my own data within a system that enables easy checking and correcting of it, as well as being able to control who buys it for what reason." • "I like the idea of having more control as it reduces or should replace the risk of fraudulent activity."	**It would make them feel more secure/more control** • "I like the idea as our personal information belongs to each of us and we should be in control of who can access it." • Ability to decide what information I release and to whom."	**It would make them feel more secure/more control** • "A better assurance of security is what I would like." • "Access to more control and visibility is a good thing." • "Being in control of my digital identity is the way life should be." • The data is mine so should be entirely in my control."
It would help reduce fraud/ scams online • "I would like to avoid being susceptible to scammers or having my email address and other data in a database traded by criminals." • I feel it would help protect against computer scammers."	**It would help reduce fraud/scams online** • "It would be great to know that my digital identity is safe and not being used for things I don't want it used for."	**It would help reduce fraud/scams online** • "Can help to reduce fraudulent activities." • "Less chances of people stealing my identity." • "Protection from scams and fraudsters."
Potential financial benefit • "Digital identity is worth money. Having ownership of it and even financially benefiting from it would be good." • "If any money is changing hands because of our data we should always get a percentage of this." • "It's my data, you want it, where's my money?"	**Help reduce fear** • "If it makes life simpler and removes fear of having my privacy invaded and my identity taken, then I would like to have more control." • "Makes us feel more comfortable using the Internet without worrying about our identity being stolen."	**Provide a one stop / simple solution** • "It would be great to have a simple, easy to manage digital identity." • "It would be good to have a one stop shop."

Figure 11 - Appeal of more personal control of our data



Source: New Zealand Digital Identity Attitudes Survey, 2022.

Table 2 - Concerns about having control of our data

2022	2020	2019
Lack of knowledge and understanding • "I would like to have more control over my digital identity but I am concerned as to what that means as far as knowledge and ability to do this." • "I would suggest that the majority of users have insufficient knowledge of the issue." • I would very much like to have more control of my digital identity but would have to receive more education to do so."	**Lack of knowledge and understanding** • "Would be easy to make a mistake if we didn't have enough knowledge." • Lack of education is a risk." • "I think it would be an excellent idea. However, luddites would need to be educated." • "I am unsure of whether or not I can manage this."	**Concern regarding loss of control and freedom** • "I don't want to end up like China." • "Dislike as I wouldn't like to end up being controlled." • "Dislike the possibility of losing personal freedoms." • "Dislike the risk of extensive government control."
Concern it would be more effort • "More control defo, as long as it doesn't mean more work, effort etc. We are pretty lazy and lax when it comes to having to jump through hoops, even for something as important as this."	**Concern it would be more effort** • "Like because you are in control. Dislike because of more admin." • "It's good to have control but I am lazy, I don't want to have to work harder." • Dislike the time and effort needed to put into more control." • "Sounds confusing and a lot of work."	**Concern regarding expense** • "I dislike the idea because it could make using the Internet cost a lot more."

Generational differences

The 2022 research has enabled us to view and identify generational differences in four cohorts; Generation Z, Millennial, Generation X and Baby Boomers.

Concerning personal information or data, Generation Z (the youngest, digital native generation) consider fewer attributes as personal information or data, while other generations tend to be more consistent with each other.

We also analysed how each cohort is currently protecting their digital identity. Generation Z is the least risk averse and their preferred tools are providing false information and disposable email addresses. Predictably, Millennials, Generation X and Baby Boomers are progressively more proactive in their risk avoidance techniques. The New Zealand results are similar to international research. Please refer to the appendix for a detailed analysis of the 2022 survey results by generational cohort.

Understanding business attitudes

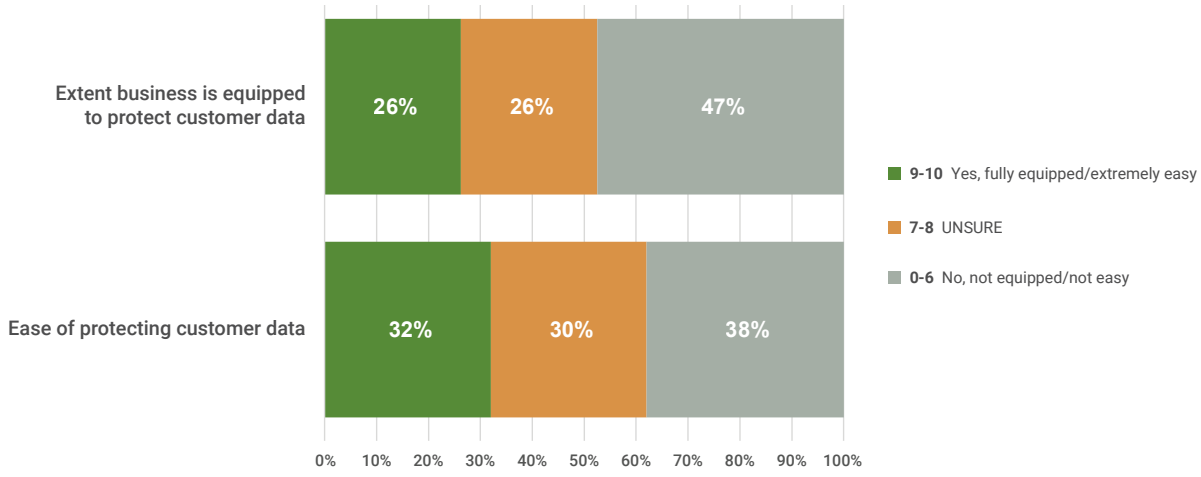
Our 2022 study also included a survey of businesses and organisations. This newly commissioned research was designed to understand the level of education, understanding and support that New Zealand businesses will need in order to adopt and make use of the CDR and DISTF impending legislation.

The survey also captures the scale of participation in the new legislation, the understanding of the value to business of this legislation and to provide insight to the level of business' understanding of the implications of DISTF and its readiness.

Survey Demographics

The Attitudes to Digital Identity Protection Obligations amongst New Zealand Businesses Survey was conducted in 2022 by Yabble Research on behalf of Digital Identity New Zealand. The survey was conducted online with a total sample of 500 respondents. Those who qualified were mainly or jointly responsible for making decisions concerning personal data protection, digital identity related fraud and unauthorised access to online accounts for the business they own or are employed by. The full methodology and sample demographics are included in the appendix.

Figure 12 - Extent businesses equipped and the ease of protecting customer data



Source: New Zealand Digital Identity Attitudes Survey, 2022.

Protecting customer data

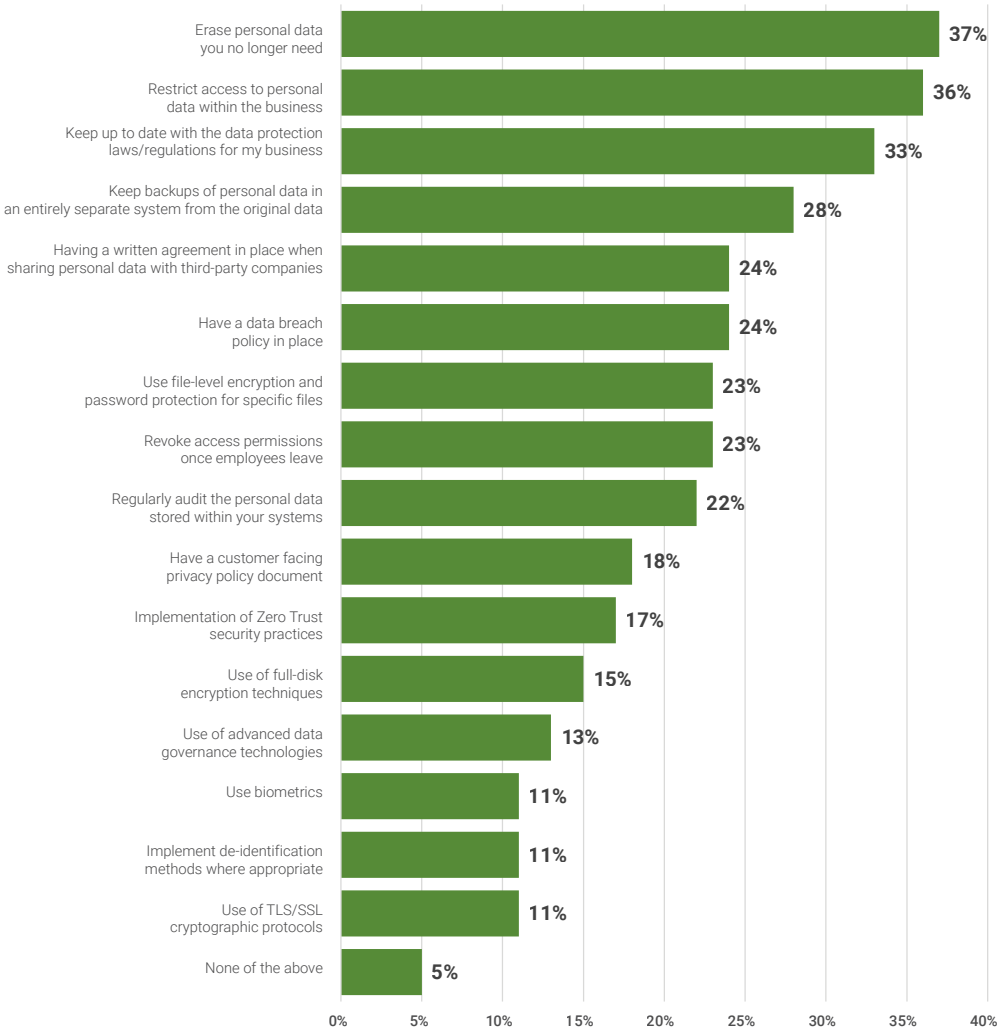
As shown in Figure 12, while 32 percent of respondents indicated that they are fully equipped to protect customer data, only 26 percent find it easy to do. Unfortunately, the majority of businesses are either not prepared to protect their customer data or unsure. Likewise, most businesses have indicated that they don't find it easy to protect customer data.

These results show how challenging it is for most businesses to operate in an increasingly digital environment.

As digital identity and consumer data right legislation is developed as many as one in five businesses indicate they do not have sufficient knowledge of the relevant legislation and their obligations. This is mainly a challenge for smaller businesses, with 90 percent of businesses with more than fifty staff indicating they are aware of the legislation.

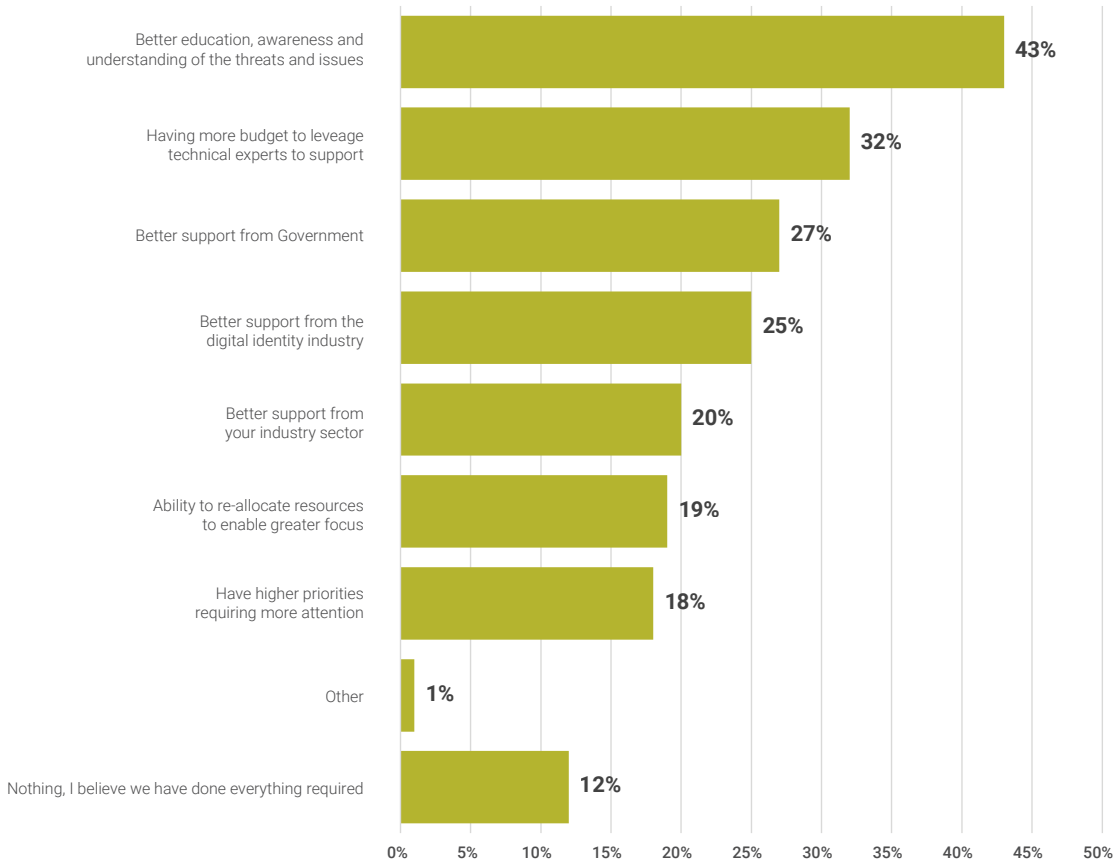
However, further analysis shows only 53 percent of respondents knew of the pending Consumer Data Right (CDR) legislation and only 39 percent the Digital Identity Services Trust Framework (DISTF). Larger businesses were much more likely to have heard about CDR (66 percent of firms with more than fifty staff) and DISTF (54 percent of firms with more than 50 staff).

Figure 13 - Measures in place to protect customers' personal identity data



Source: New Zealand Digital Identity Attitudes Survey, 2022.

Figure 14 - What would improve business data security



Source: New Zealand Digital Identity Attitudes Survey, 2022.

Nevertheless, this shows that while most businesses assume they know their obligations, many do not. This reinforces the need for improved communication and education for businesses to better protect their customer data.

Cybersecurity and data protection

Cybersecurity, hacking and loss of customer data continue to feature regularly in the headlines yet almost half (49 percent) of all businesses have not sought any advice on cybersecurity or data protection in the past twelve months.

There is a stark difference between large and small businesses when it comes to cybersecurity. While 60 percent of businesses with more than 50 staff have sought advice in the past 12 months, only 35 percent of businesses with less than 50 staff have.

When asked what measures the business has in place to protect customers' personal identity data a broad range of approaches were described. However, as can be seen in Figure 13, most security measures are under utilised by businesses. The most common security measure was the erasure of customer data when no longer needed and this is only carried out by 37 percent of businesses.

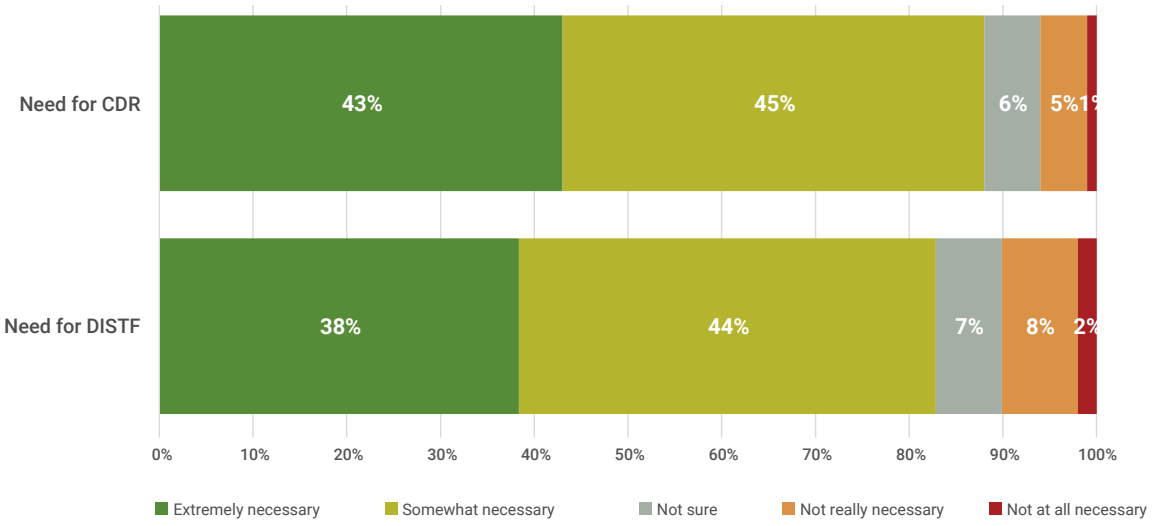
Meanwhile, as shown in Figure 14, four in 10 businesses believe better education of their workforce and increasing awareness/ understanding of threats would help further protect and manage personal identity related data. A quarter of respondents believe that more support from the digital identity industry would help improve data security. A surprising 12 percent of respondents believe that they have done everything required to protect their customers' data.

Thoughts about regulation

The nature of threats and the opportunity costs has created an environment where most businesses believe that regulation is necessary. As can be seen in Figure 15, 88 percent of businesses believe the CDR regulations are necessary and 82 percent believe a DISTF is also necessary.

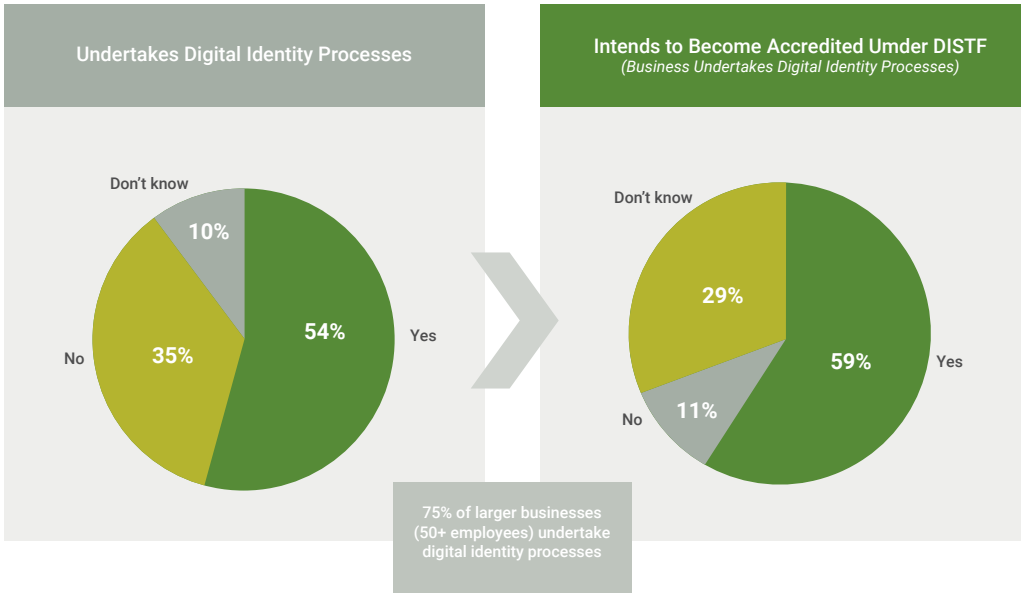
Of those currently engaged in digital identity processes, 59 percent intend to become DISTF accredited (Figure 16).

Figure 15 - Is regulation necessary?



Source: New Zealand Digital Identity Attitudes Survey, 2022.

Figure 16 - Do you intend to be accredited under DISTF?



Source: New Zealand Digital Identity Attitudes Survey, 2022.

PART THREE: Opportunities, Challenges and Recommendations

Our Global Market Opportunity – Exporting Trust: New Zealand as a Trusted Economy

Aotearoa New Zealand is seen as a highly trusted and low corruption country globally. Alongside Denmark and Finland, New Zealand is equal number one in the world in the International Transparency-Corruption Perceptions Index. In a world where there is an ever growing threat of cyber crime and identity theft the ability for Aotearoa to position itself as a trusted economy is a differentiating factor for New Zealand companies in digital trade globally.

Aotearoa has a unique advantage due to its size and focus on inclusive and equitable outcomes for all, to be at the forefront of creating a trustworthy digital economy - not only domestically to advance its social and economic goals, but also internationally for the growth of digital trade.

During the 2022 Digital Trust Hui Taumata conference, the panel discussion Global Opportunities for New Zealand as a Trusted Economy, explored these opportunities.[10] The mahi and outcomes identified in the Digital Strategy for Aotearoa, in particular the Digital Technologies Industry Transformation Plan, the Digital Commerce Programme, Digital Trade and the enactment of the Digital Identity Services Trust Framework are important steps in continuing to grow our international trade in the digital economy.[11]

Privacy-respecting digital identity is an essential foundation for building trust. As interoperability and cross recognition of the Digital Identity Services Trust Framework (DISTF) advances towards reality in our trading markets, services that leverage accreditation and certification may gain international opportunities.

The Digital Economy Partnership Agreement (DEPA)[12] is an example where cross border trust is already operating. The DISTF could remove further friction. In the coming years we will see a proliferation of digital trade agreements where the trustworthiness of a nation's service providers will become a critical success factor. In time, once legislation and supporting compliance are aligned across various borders, offshore customers will be able to know that they are dealing with a trusted New Zealand business, and vice versa.

For example, an NZUS Council study shows there are few barriers to entry into some offshore markets. Where supported by policy and technically interoperable digital trade agreements, "the trustworthiness of digital services from Aotearoa can shine through brighter than competitors from other countries.[13]"

Spark subsidiary MATTR is a recent example of a locally established New Zealand based digital identity company now operating globally. Another example is APLYiD in the financial services market. These examples indicate the trustworthiness of New Zealand's digital identity service providers in offshore markets.

Challenges to growing a local digital identity sector

Aotearoa New Zealand's experience broadly reflects that seen in other common law jurisdictions that have no national ID card and a market is allowed to emerge for digital identification, authentication and authorisation

to access services. Underlying architectures and the services built on top of them are largely based on international standards - not because there is regulatory pressure to do so, but because it is expedient so as to assist a service's interoperability with other systems in the domestic market and overseas. A non-exclusive list of the most recognised challenges is shown below.

Small market scale

The small scale of the local New Zealand market is a factor in almost all market analysis of the economy. The relative lack of investment capital also impacts innovation domestically. These factors also apply to the highly competitive digital identity market. Approximately 10 years ago, a small group of companies began operating in New Zealand providing digital identity services. While small, the market has been progressively growing with an increasing number of international companies entering the market.

SMEs and the public sector

The public sector market, a significant purchaser of identity services, can be particularly challenging for startups and SMEs. Smaller local firms can be edged out by multi agency public sector licence deals which tend to favour larger organisations.

RealMe's impact on the market

Another challenge for some SMEs has been the perceived market dominance of RealMe. It is the established public facing digital identification and authentication service and being publicly funded together with an expectation that public service agencies at least offer it as an option, is less susceptible to market forces with requisite pros and cons. However, funding limitations hamper its ability to fulfil all market needs across all sectors at all levels of robustness dependent on the identity - related risk inherent in the transaction, which has led to the

emergence of local and international providers catering for sectors and niche markets in New Zealand typically as white labelled services.

RealMe has an additional advantage being operated by the Department of Internal Affairs' (DIA) Service Delivery and Operations Branch. This is the agency that holds the registers of authoritative sources of people's personal information such as Births, Deaths, Marriages, Passport details and more. The agency enables RealMe to verify personal information claims of its own and partners' customers directly. In contrast, other agencies and the private sector require agreements with DIA to achieve a similar outcome, for example, CentraPasses's Kiwi Access Card (18+).

Budget 2022's $83 million (over four years) funding announcement for RealMe may change this dynamic. While the majority of the funding is expected to contribute to RealMe's year to year operating costs, it is hoped that some funding will be directed to the modernisation of the systems described above. RealMe has stated that it intends to publish a white paper on this topic, specifically on technology agnostic platform evolution, strategic architecture, and API-Gateway for a flexible and extensible verifiable credential ecosystem, an ecosystem in which both the public and private sectors invest, innovate, and thrive in a digital economy for Aotearoa New Zealand.

The overall effect of these dynamics rebalances the perception of RealMe's crown-funded market dominance vs equitable partnership with the private sector, which may eventually invigorate the much-needed confidence and trustworthiness in Aotearoa's digital economy. This is accomplished through the implementation of a strategic policy-led approach to improving the overall security, privacy, and data protection of people's personal information when conducting digital services and transactions online.

Success stories

Spark's creation and development of its subsidiary MATTR is a notable example. Their early technical understanding of the emerging architectural option of decentralised digital identity in advance of many players enabled it to deliver decentralised identity solutions at scale around the world. Domestically, MATTR along with JNCTN, another local tech startup, developed solutions to support New Zealand's response to the pandemic. JNCTN focussed on the identification, onboarding and credential management of the 16,500 personnel working in the managed isolation and quarantine facilities run by the Ministry of Business Innovation and Employment (MBIE), while MATTR built public-facing digital solutions for the Ministry of Health.

Another SME example is APLYiD, which has received Series A funding for its digital identity innovations in the financial services market[14].

Together MATTR, APLYiD and JNCTN show where Aotearoa's SMEs have identified niches and taken global leadership positions.

Key Recommendations

The essence of Digital Identity New Zealand's vision and mission is to foster an environment where people can trust digital identity service providers that enable equitable access to digitally delivered services. This in turn will enable increased participation in the digital economy, ultimately helping to lift prosperity and wellbeing for all.

This research highlights that the issues holding back more rapid uptake of digital identity and hence the growth of the digital economy have remained consistent for the past four years. These issues stem from a lack of trust, understanding and confidence. Consequently, Digital Identity New Zealand provides the following recommendations, distilled from the research, to support the collaborative improvement of the Aotearoa digital identity ecosystem.

1 THEME ONE - **Build trust**

The challenge: Due to a poor experience, misinformation or otherwise, a statistically significant number of people in Aotearoa do not trust digital identification or digital services.

Recommendations:

1.1 The Government must encourage businesses to pursue multiple avenues to demonstrate trusted services for the public.

- The Government must actively encourage online services providers to be accredited under the Digital Identity Services Trust Framework (DISTF) Act (as soon as it is passed into legislation and the rules are confirmed).
- The Consumer Data Right (when it emerges) and the Office of the Privacy Commissioner's Trust Mark are other potential frameworks that digital identity service providers must be encourage to engage with to build consumer trust in their online services.

1.2 Businesses must actively participate in frameworks available to create and demonstrate trust.

- The DISTF Act, the Consumer Data Right and the Office of the Privacy Commissioner's Trust Mark are three 'demonstrations of competency' that digital identity service providers should consider to build consumer trust in their online services.
- To further increase an environment of trust, online service providers should consider engaging with additional credible third party schemes and awards to build people's trust in the integrity and quality of their service.

Broader than digital identity services specifically, there is an opportunity to motivate excellence in the provision of digital services through greater promotion of ISO 27001 certification and similar global information security certifications. Awards offer another avenue of motivation. Excellence in IT Awards (IT Professionals NZ), iSANZ Awards (Information Security in New Zealand), Bestawards.co.nz/Digital (Design Institute) and others should be better promoted and entries encouraged. They could be augmented by the addition of a category for digital identity services.

1.3 Businesses and Government agencies must increase their investment in security measures that protect customer information, and in cybersecurity in general.

- The research shows most security measures are under utilised by businesses. Where carried out, the most common measure (erasure of data) is carried out by less than four in ten.

Information Privacy Principle 9 of the Privacy Act 2020 states: "An agency that holds personal information must not keep that information for longer than is required for the purposes for which the information may lawfully be used." Some sector specific laws do stipulate periods of collection and storage but beyond these, the organisation has the responsibility to erase personal information as soon as it no longer needs it. In many cases this is soon after its collection and verification. The risk of exposure, breach, litigation and brand reputation increases each day that data is held. Organisations should undertake regular audits of the personal information it holds, undertake a Privacy Impact Assessment to understand the risks of holding it, and have clear policies for erasure at the earliest opportunity afforded by the results of the Privacy Impact Assessment.

- Online service providers should amplify the message that online security and data protection is a shared responsibility.
- The Government should increase overall investment in the promotion and implementation of cybersecurity for agencies and citizens.

2 THEME TWO - **Increase education and understanding**

The challenge: There is an acute lack of public understanding regarding digital identity, why it is important, and how they can better protect their identity online. Despite significant efforts by CERT NZ, NetSafe and others, messages don't reach some of the most vulnerable in society.

Recommendations:

2.1 The Government should help develop best practice guides for service providers to help them educate users visiting their sites.

- Currently, a range of techniques are available to help people in their digital service experiences, but are not used consistently. The techniques should be collated into a single suite of guidance that form a component of conformity assessment for the DISTF, website awards and similar recognition of achievement.
- The Government could also help develop simple and accessible education regarding password manager services, password construction and good security/anti-fraud habits.

2.2 Businesses must improve the provision of security information and education for users on their web pages.

- Landing web pages for transactions or access to services should carry reminders, hints and links to good practice, either developed by the online service itself or to external content such as CERT NZ.

2.3 Businesses and Government agencies must increase investment in the education of their own staff with respect to protecting their customers' data.

- As noted in Part One, four in ten businesses believe better education of their workforce and increasing awareness/understanding of threats would help further protect and manage personal identity related data.
- As part of an organisation's commitment to raising the bar on its competency and capability in respect to the provision of digital identity services, a specific budget should be allocated to support this objective.

3 THEME THREE - **Drive confidence and engagement**

The challenge: Digital identity and cybersecurity are often seen as complex issues that can make the online experience more daunting. Now that more digital services are provided requiring identity and security, many lack the confidence to fully engage.

Recommendations:

3.1 The Government should ensure that identity services cater for all sectors of society and that all sectors of society have the skills and confidence to engage with these services.

- Digital exclusion has many causes, but confidence to engage with digital services is one of the recognised challenges. The Government must invest in addressing digital exclusion, including helping vulnerable cohorts.
- The Government has a responsibility to ensure that digital services are available for Māori respecting Te Tiriti o Waitangi and the te ao Māori worldview.

3.2 Businesses must develop their online presence in ways that make it easier for people to understand how to protect their personal information in culturally appropriate ways.

- Businesses should take into account the diversity of the Aotearoa New Zealand market and provide information about how they protect each of their potential customer cohorts data. Businesses should provide simple notices on websites or forms where a user action will result in the processing of personal data. This helps raise awareness and educate people of the implications of divulging personal information while benefiting from a digital service.

3.3 Businesses and Government agencies should be encouraged to use plain language summaries of their key messages such as privacy statements and user agreements.

- Privacy notices are typically written by lawyers and the language used can overpower people's ability to understand them. Writing 'plain language' summaries help educate people as to the essential points of the notice, while not taking away the legal position that the formal notice carries.

4 THEME FOUR - **Develop the Digital Identity sector**

The challenge: Achieving a strong, consistent and sustainable level of data protection policy in the face of a severe IT skills shortage and commercial expediency. There is a risk that the focus is simply on compliance rather than the development of a country wide culture of protecting people's personal information.

Recommendations:

4.1 The Government should encourage service providers to also look toward non legislative best practices regarding personal information protection, processing, storage and deletion.

- Businesses should be encouraged to audit current practice to set a baseline for improvement with requisite goal setting.
- Auditing of current practice should be undertaken at an organisation level to benchmark the current state, in order to set goals for improvement over time.

4.2 Businesses should appoint a data security lead, or a role that oversees data security and privacy.

- Organisations need to reflect the transformation of their services to the digital channel for delivery, with a fit-for-purpose organisation structure.
- In larger organisations, the Board should appoint people to Chief Information Security Officer (CISO) and Chief Privacy Officer (CPO) roles. These roles should report regularly to the Board for a direct line of sight.

4.3 Businesses and Government should collaborate with Digital Identity New Zealand to create a national culture of best practice for protecting people's information online.

Appendix

Research Methodology

Survey #1: Understanding attitudes to Digital Identity among New Zealanders (General Public/Consumer Research)

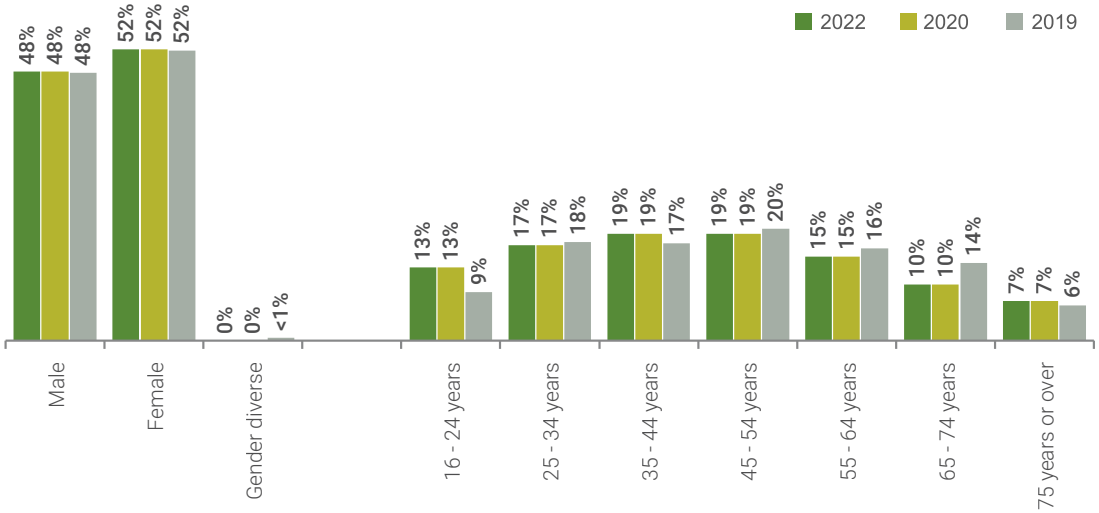
Digital Identity New Zealand has undertaken annual research on consumer understanding of digital identity, personal data and trust since 2019. This research has been conducted each year by Yabble, one of New Zealand's leading data and insights businesses.

The 2022 Consumer Digital Identity research was conducted between 29 June to 18 July, 2022. Previous years research was conducted across June/July 2020 and through April in 2019.

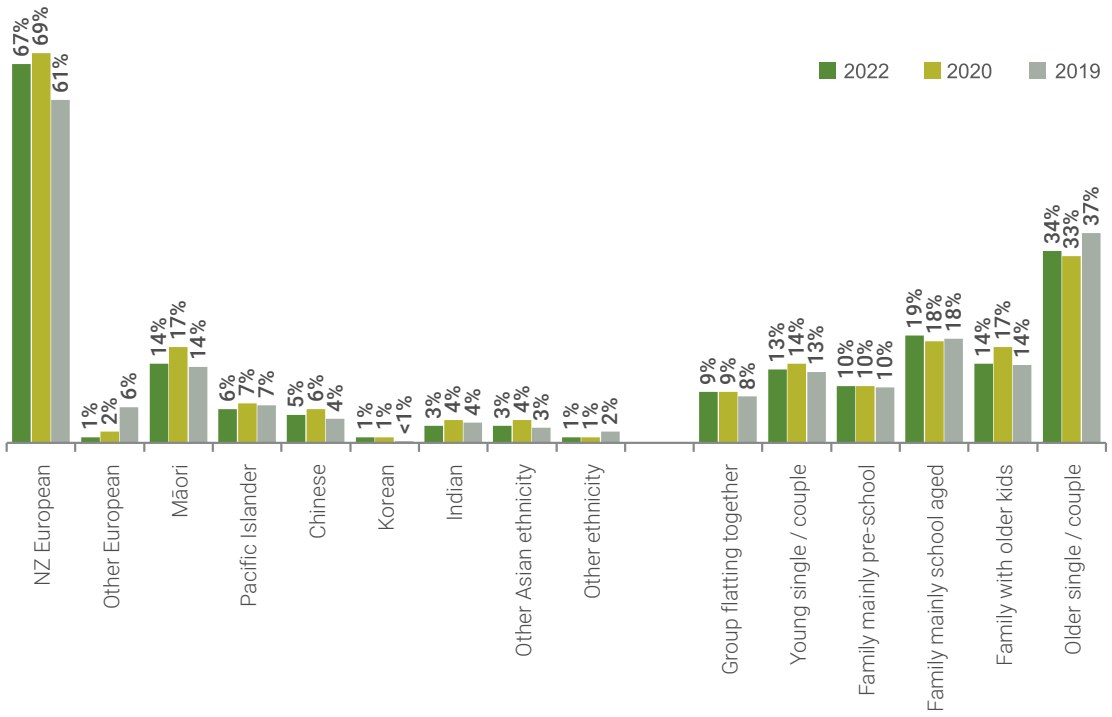
The 2022 study was designed to uncover new issues, opportunities and barriers as well as benchmark changes in sentiment and behaviour between 2022 and the previous years.

The survey was conducted online with sample sizes to allow for representative samples by age, gender, ethnicity and location. The fact that these surveys were conducted online introduces some inherent bias missing a segment of the community that is not digitally connected.

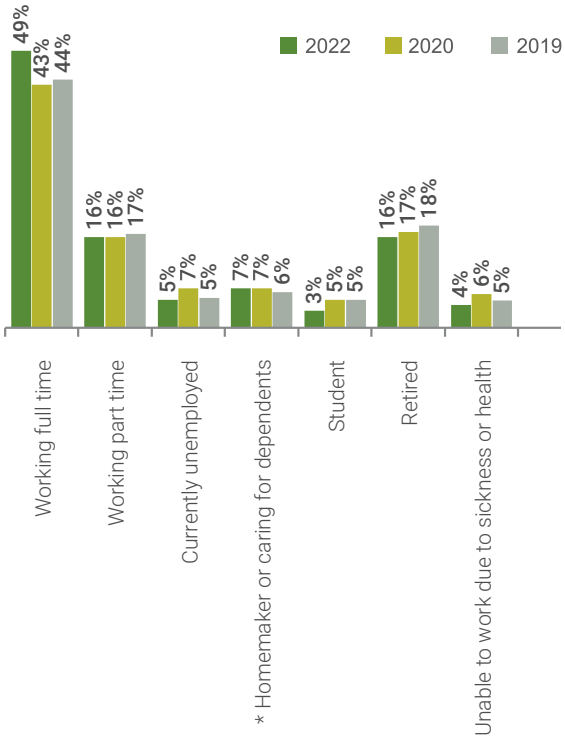
Survey sample sizes: 2022: N = 795, 2020: N = 1,011, 2019: N=1,092



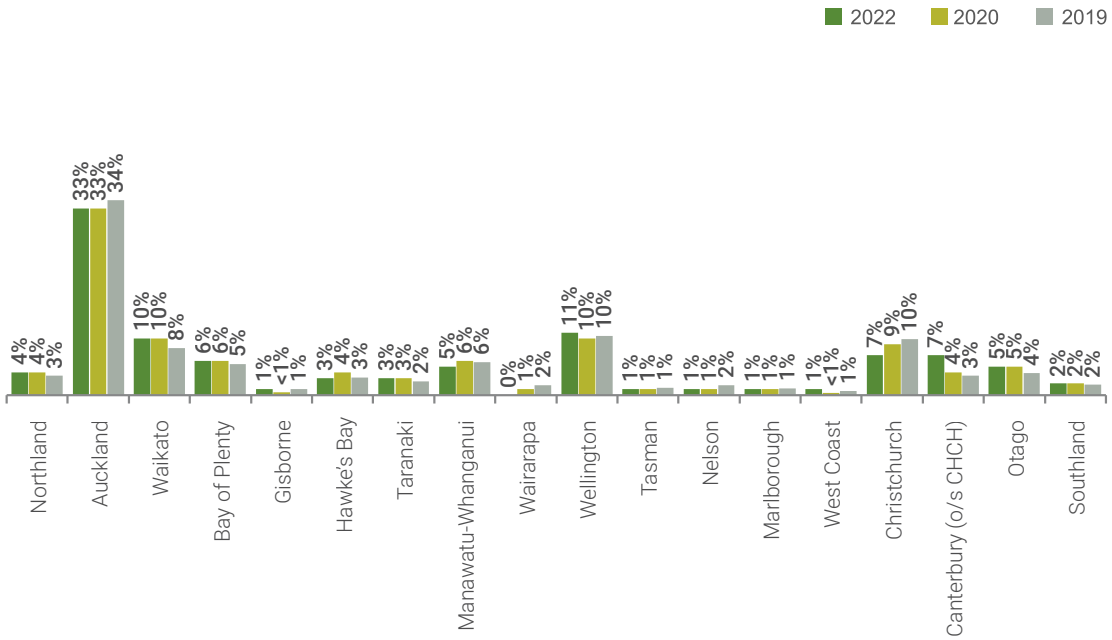
Age / Gender



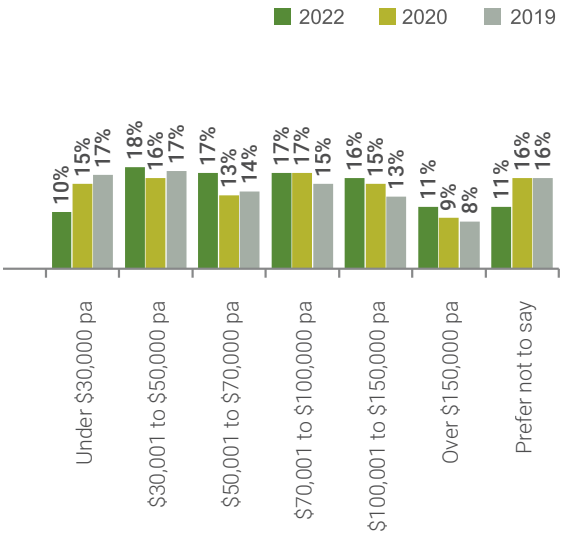
Ethnicity / Household



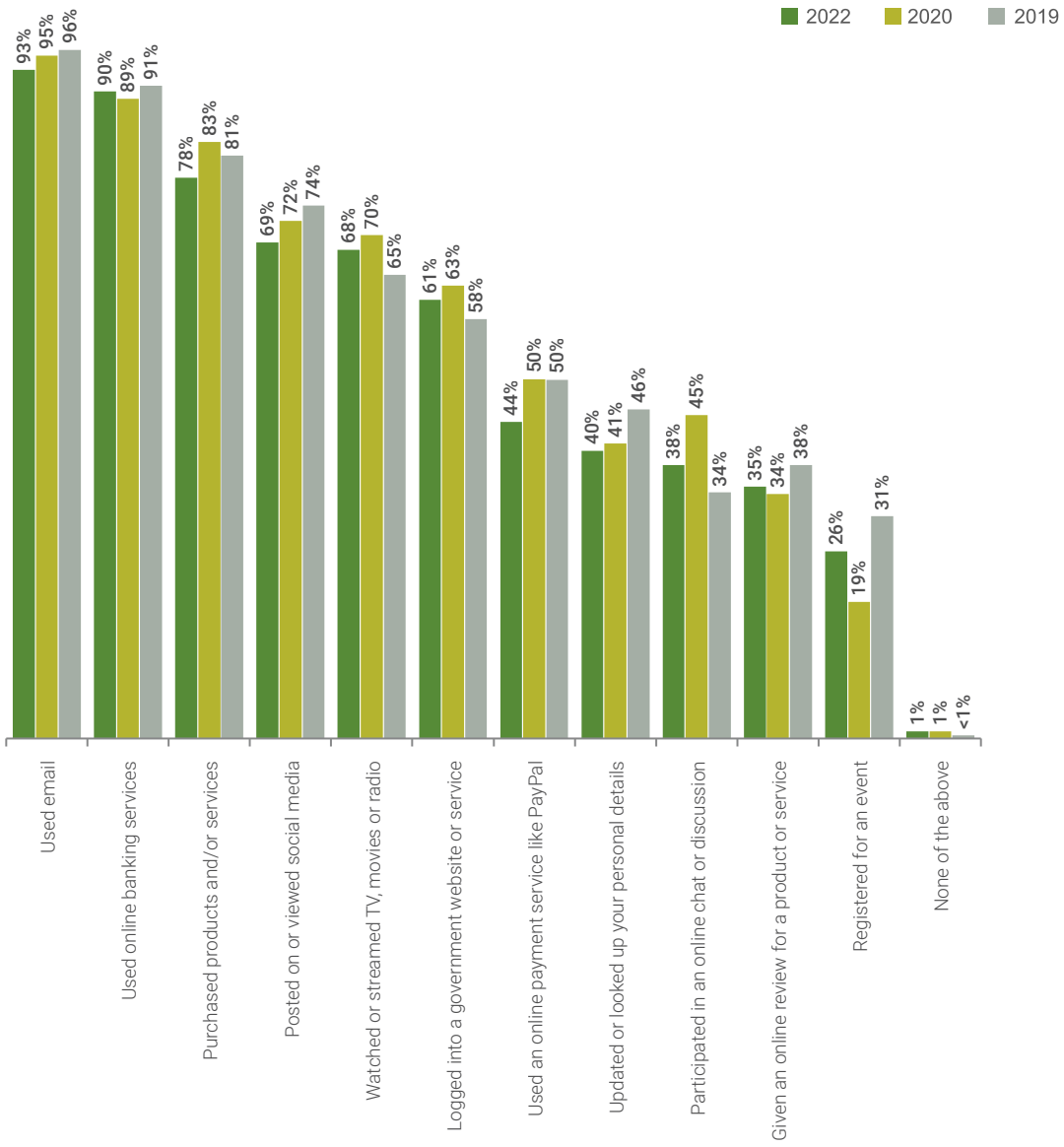
Employment status



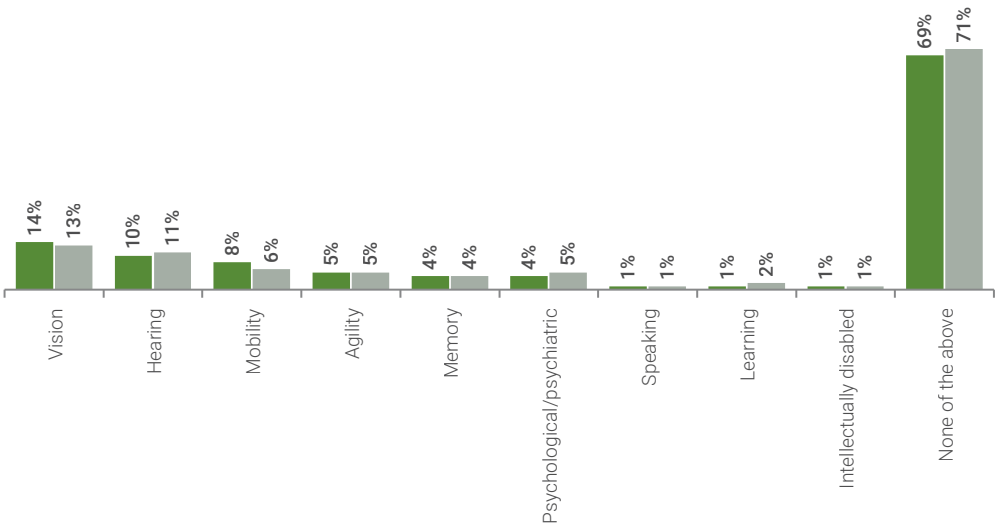
Region



Household income



Done online in the last three months



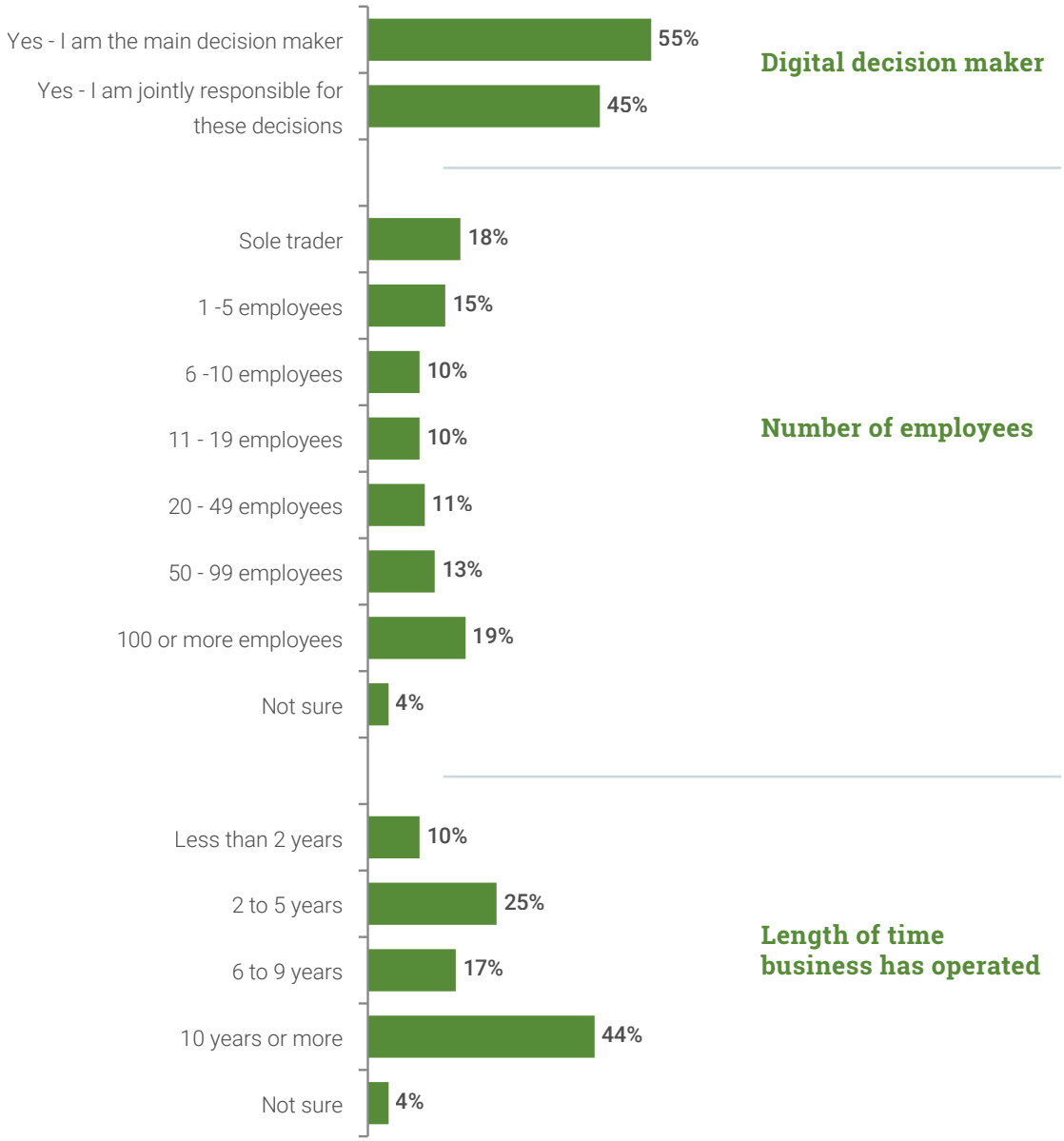
Disabilities/impairments

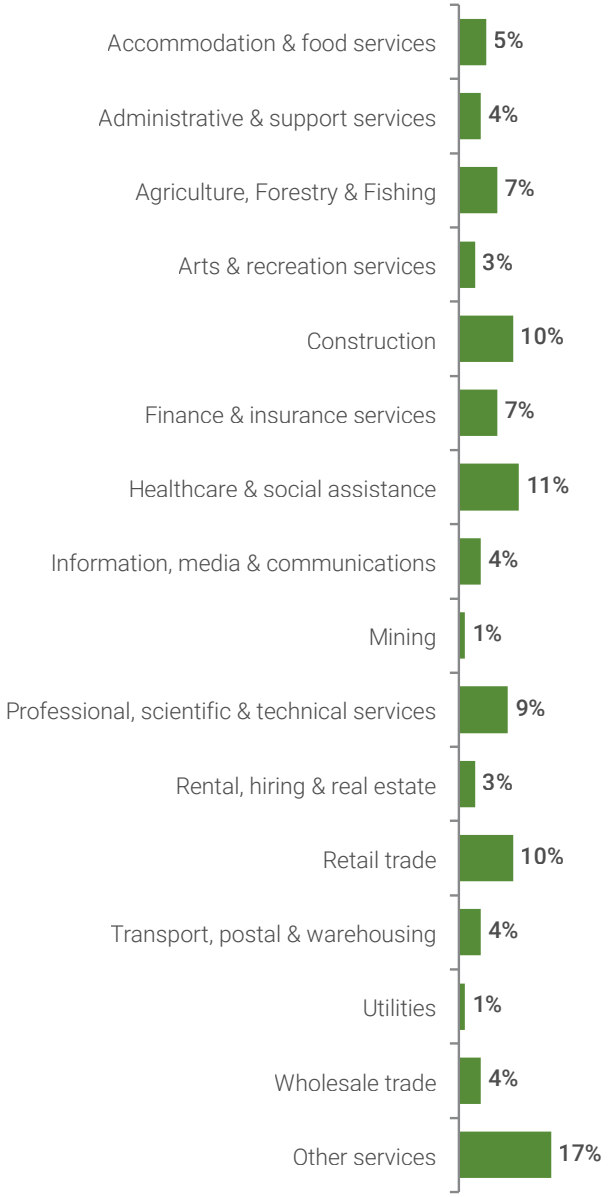
Survey#2: Understanding attitudes to Digital Identity Protection Obligations amongst NZ Businesses

All respondents screened to ensure mainly/jointly responsible for making decisions about online digital protection

Survey sample size. Base Total: 2022 N=500

Q. Are you responsible for making decisions about protecting personal data, digital identity-related fraud and unauthorised access to online accounts in your business for the business you own or are employed by? Q. How many employees does your business/organisation have? Q. How long has your business been operating? | Q. Which of the below industries best reflects your business?

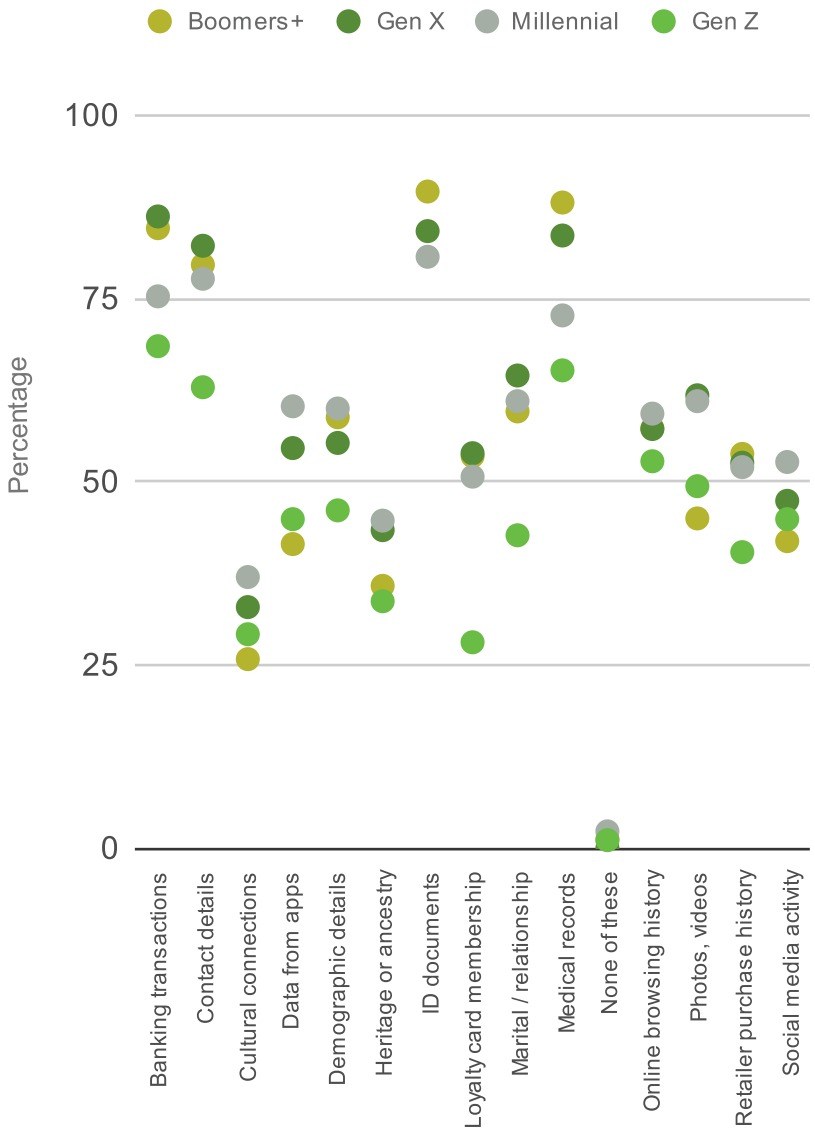




Industry that best reflects business

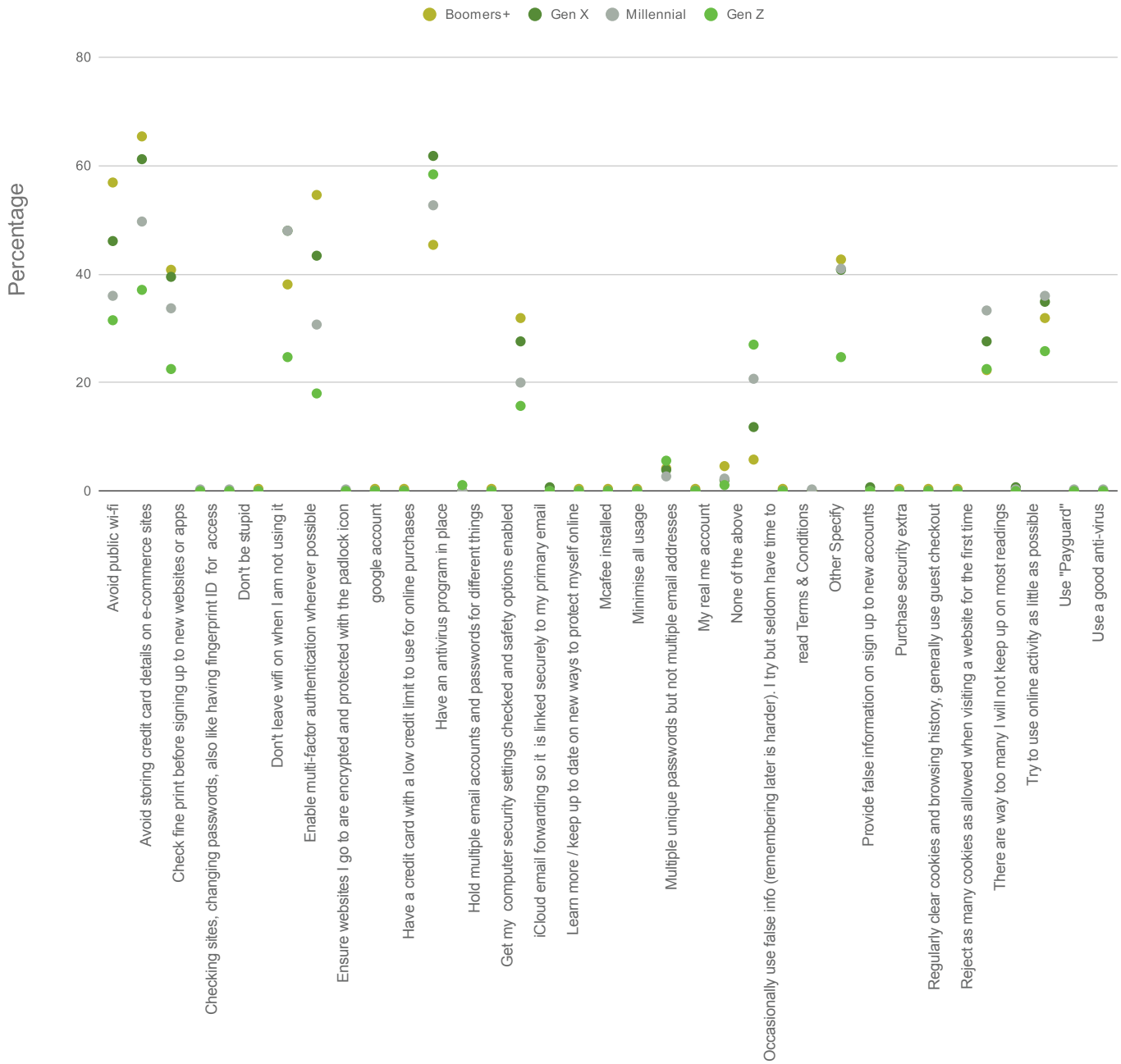
We took the age breakdown of the respondents and grouped them into four generational categories - and applied the categories to the questions. There were some interesting (surprising!) results from some questions. Those are summarised in the following:

Which if any do you consider to be your personal information or data?



Gen Z (the youngest, digital native generation) tends to consider fewer things as personal info / data, while the other three generations tend to be more consistent with each other:

Which of the following do you currently do to protect your digital identity online?



Gen Z is the least risk averse, and their tools are providing false info and disposable email addresses. Predictably, Millennials, Gen X and Boomers+ are progressively more proactive about their risk avoidance techniques.

Further analysis of this topic can be found in this eBook from Mitek: https://www.miteksystems.com/innovation-hub/research-reports/bridging-digital-identity-generational-gaps

References

1. Identification Terminology, Digital.govt.nz, Department of Internal Affairs. Accessed October 2022. https://www.digital.govt.nz/standards-and-guidance/identification-management/identification-terminology

2. Digital Identity Guidelines, National Institute of Standards and Technology Special Publication 800-63-3, US Department of Commerce. June 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

3. Digital Identity Use Cases, Digital Identification and Authentication Council of Canada. Accessed October 2022. https://diacc.ca/digital-identity-use-cases/

4. Digital identification: A key to inclusive growth, McKinsey Global Institute. April 2019. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

5. Govt helps to protect New Zealanders digital identities. News Release, Beehive.govt.nz. October 2021. https://www.beehive.govt.nz/release/govt-helps-protect-new-zealanders-digital-identities

6. Ensuring socio economic inclusion through digital identity, Global Voice Group. March 2022. https://www.globalvoicegroup.com/news-article/ensuring-socioeconomic-inclusion-through-digital-identity/

7. Inclusive and Ethical Use of Digital Identity Working Group Discussion Paper, Digital Identity NZ. April 2022. https://digitalidentity.nz/inclusive-and-ethical-uses-of-digital-identity/

8. Digital identity verification spending to pass $20B by 2027, but security challenges remain, Biometric Update.com. August 2022.

9. Minister launches online gateway to govt services, New Zealand Government Media Release, December 2009. https://www.beehive.govt.nz/release/minister-launches-online-gateway-government-services

10. Digital Trust Hui Taumata, Digital Identity New Zealand. August 2022.

11. 2022–23 Action Plan for the Digital Strategy for Aotearoa, Digital.govt.nz, 2022. https://www.digital.govt.nz/dmsdocument/238~202223-action-plan-for-the-digital-strategy-for-aotearoa/html

12. Digital Economy Partnership Agreement (DEPA), Ministry of Foreign Affairs and Trade, NZ Government. https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/

13. Barriers to NZ-US Digital Trade - Are there any?, NZUS Council, October 2001. https://www.nzuscouncil.org/wp-content/uploads/2021/09/FINAL-NZUS-DIGITAL-EXPORTERS-web-1.pdf

14. APLYiD Secures NZD$7M in Series A Funding, FINSMES. October 2021. https://www.finsmes.com/2021/10/aplyid-secures-nzd7m-in-series-a-funding.html

DIGITAL IDENTITY.NZ

Phone: +64 9 394 9032 **info@digitalidentity.nz**
www.digitalidentity.nz

DIGITAL IDENTITY NEW ZEALAND
c/o NZTech
PO Box 302469
North Harbour Auckland 0751

@digitalidnz digitalidnz @digitalidnz