

# Built to succeed: Resilience in the age of disruption, cyber risk and AI

## A survey of 400 Kiwi businesses

# Foreword

## New Zealand's resilience is a joint responsibility

New Zealand businesses have been tested repeatedly in recent years. A global pandemic, extreme weather events and more recently geopolitical conflict, have all added pressure to doing business.

Business risks are also becoming more interconnected. A weather event can interrupt power, connectivity and transport. A network outage can stop access to cloud applications and payment systems. A compromised account can become a wider cyber incident. And poor data governance can undermine the successful adoption of AI.

Against this backdrop, resilience is a core business capability. It's what allows an organisation keep serving its customers, protect its people and data, adapt to change and keep investing in its future.

> *New Zealand's economic resilience rests on the capabilities of thousands of individual businesses.*

### The role of individual firms

New Zealand's economic resilience rests on the capabilities of thousands of individual businesses. Resilient firms go beyond the ability to endure disruption to a capacity to respond, recover and adapt. Businesses that do this well are more deliberate about investment planning. They build stronger foundations across their people and technology, including connectivity, cloud environments, cyber security and data.

Our research shows that while many New Zealand businesses recognise the threats, only 16% have resilience plans they regularly review to test their preparedness. By contrast, three-quarters of the businesses that rate themselves most highly for both productivity and growth confidence have documented resilience plans.

### The role of Government

Government has an important role in providing clear policy settings, strengthening national infrastructure and cyber capability, supporting skills development and helping communities prepare for natural hazards. But Government can't do it alone. Business leaders must understand their own critical dependencies, remove single points of failure, protect their systems and regularly test whether their organisation can continue operating when something goes wrong.

### Spark recognises its role

At Spark, we recognise that connectivity is an essential service, and investing in our network is a key priority so that we can continue to provide reliable and resilient connectivity to businesses and households across New Zealand.

> *Resilience goes beyond the ability to endure disruption to the capacity to respond, recover and adapt.*

This report is intended to help businesses take practical action. It identifies what contributes to a business' resilience and considers what some of New Zealand's most confident and productive businesses are doing differently.

Businesses today should view resilience preparedness as a cost to be managed, but an investment in continuity, confidence and future growth. The stronger and more adaptable our businesses become, the better equipped New Zealand will be to withstand the next disruption and make the most of the opportunities that follow.



**Mark Beder**
Spark Chief Customer Officer – Connectivity

# Contents


**Foreword** ..... 2

**Research summary** ..... 4

**Business resilience plans** ..... 5

SECTION 1

**Resilience planning** ..... 5

SECTION 2

**Resilience capability** ..... 8

SECTION 3

**Resilience enablers** ..... 10

- Connectivity ..... 10
- Cyber security ..... 12
- AI adoption ..... 16
- Data storage ..... 19

SECTION 4

**Resilience actions** ..... 21

**Endnotes** ..... 22



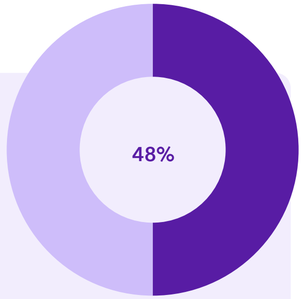

# Research summary

A total of **404 New Zealand business leaders** were surveyed between 21 August and 5 September 2026, to understand how New Zealand businesses view resilience in the context of their own business. Detailed findings are set out in this report; the key findings are summarised below.

**Just 44%** of Kiwi businesses surveyed have developed a **resilience plan**, and **only 16%** regularly review or test the plan they have.

Businesses **investment to improve resilience** has mainly focused on upskilling staff **42%** over secure cloud backups and data recovery **31%** or connectivity for remote working.

## Almost half (48%)




of businesses have experienced a **cyber security incident**, rising to **58%** among businesses with 100+ employees.

Yet only **54%** have a **formal password policy**. Fewer still provide regular phishing training **(39%)** or have policies governing staff use of AI **(33%).**

**Connectivity under-prioritised.** Seven in 10 businesses haven't got their basics right to enable consistent connectivity, yet only **16%** would prioritise investment in network infrastructure if given money to grow.

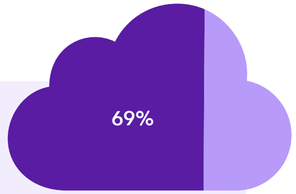
## AI use is mainstream, but advanced adoption is still limited

- 69% use AI to some extent, most commonly general purpose chat tools.
- Only 15% use semi- or fully autonomous AI workflows.

## Data foundations may constrain the next stage of AI adoption

- **26%** mainly use siloed data for reporting.
- Just **21%** have unified data and AI embedded in business processes.

## Cloud is the main home for business-critical data




**69%** have this stored with an international or local cloud provider. The lack of **cloud backups** is also an area of risk. Only **31%** invested in secure cloud backups and data recovery to improve their business resilience.

**A more resilient pattern emerges among** *Confident performers***.** This group—businesses rating themselves 9–10 for both productivity and confidence in meeting their growth ambitions—represents about **9%** of the sample.

**Nearly half (49%) of** *Confident performers* have documented and regularly reviewed resilience plans. They're also more likely than businesses overall to have policies governing AI use (**58% vs 28%** of all businesses), prioritise investment in improved cyber security (**45% vs 19%**).

This is the second report in Spark's series on New Zealand business performance, following the 2025 report *Lifting productivity: Moving New Zealand from getting by to getting ahead.*[1]

SECTION 1

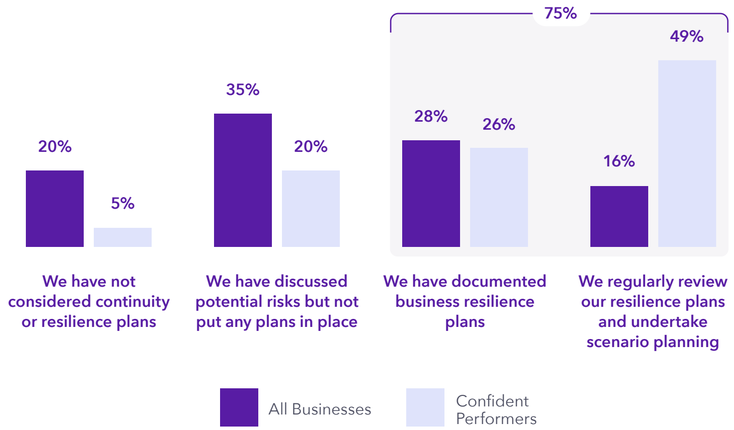
# Resilience planning

Many Kiwi businesses are unnecessarily exposed. Around half have no resilience plan and fewer still have put theirs to the test.

New Zealand businesses must have strong coping mechanisms to succeed in an environment where global incidents, network outages or local weather can unsettle business as usual. Yet, for many, resilience remains an informal discipline. Our research found that less than half (44%) of all businesses have made business resilience plans. Only 16% of businesses review their plans regularly. In contrast, 75% of *Confident performers* have documented business resilience plans.

## Business resilience plans

### Fewer than half have business resilience plans




Q To what extent has your organisation done any planning to improve its ability to prepare for and respond to a possible future events? (categories mutually exclusive)

**Spark view: Connectivity is core to resilience**

*Many businesses set up remote working in a hurry, often as a stopgap. We still see organisations running their entire operation over a single connection, with no backup if it fails, and staff connecting from home. Connectivity tends to be invisible until everything grinds to a halt. Businesses that handle disruption well have planned for disruption – they have backup connectivity and can switch to it without a hitch, and they treat secure access for remote staff as part of their core infrastructure.*

– **Sam Thumath**, GM Business Connectivity

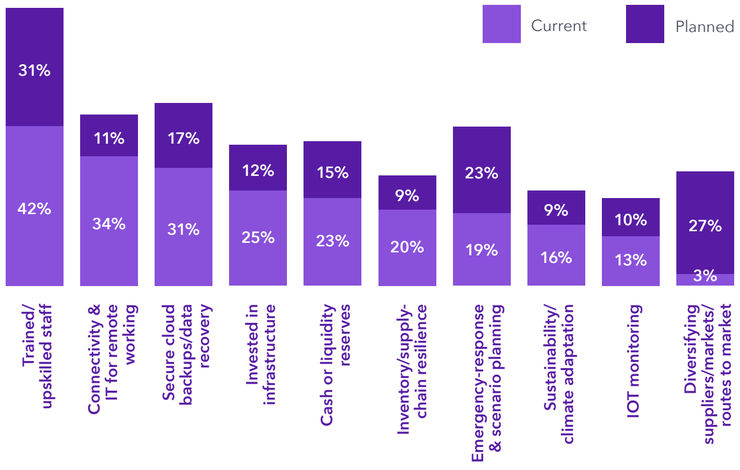


## Investment to improve resilience

While resilience appears to be an informal discipline in many businesses, they're at least recognising the need to be more resilient. We asked the businesses where they have invested to improve resilience. In the last year this had included upskilling staff (42%), connectivity and IT for remote working (34%) and secure cloud backups and data recovery (31%).

Staff training is the biggest focus for the next 12 months (31%), closely followed by an intention to diversify suppliers and markets (27%). Encouragingly, 23% say they want to invest in emergency response and scenario planning in the next year.

### Most businesses key focus for resilience is staff training




Q Thinking about last 12 months which of the following has the business invested to improve its resilience?

Q And which, if any does it plan to invest in over the next 12 months to improve its resilience? (Choose all that apply)



CONFIDENT PERFORMERS

## Who are the *Confident Performers*?

Defined as businesses that **score 9 or 10 in rating their organisation's productivity and 9 or 10 in confidence the organisation will meet its growth ambitions**. *Confident performers* are more concerned about capability rather than survival.

- Technology is at the heart of these organisations, with 87% stating that up-to-date or advanced technology is critical to their business.
- 59% regard international sales as critical or important to the business.
- 64% are established businesses and 36% are start-ups or new businesses in growth phase.
- This group prioritise investment in technology to achieve further growth, with workforce talent second.
- Higher use of more advanced AI, with 27% using semi or fully-automated AI agentic workflows (compared to 15% of businesses overall) and only 8% saying they aren't using AI at all in their business.

Government sets the conditions for New Zealand's resilience, funding critical infrastructure, setting regulation and providing emergency information and support to help firms survive shocks.

## NZ Cyber Security Strategy

IT resilience is recognised as a core pillar of the country's economic and national security in the New Zealand Cyber Security Strategy 2026–2030, released in February 2026.[2] The document shows a shift in the country's historically "light-touch" digital guidelines toward tighter regulation and enforcement. While 71% of businesses surveyed are aware of the Strategy, only 16% have read it, highlighting an opportunity to increase awareness and education.

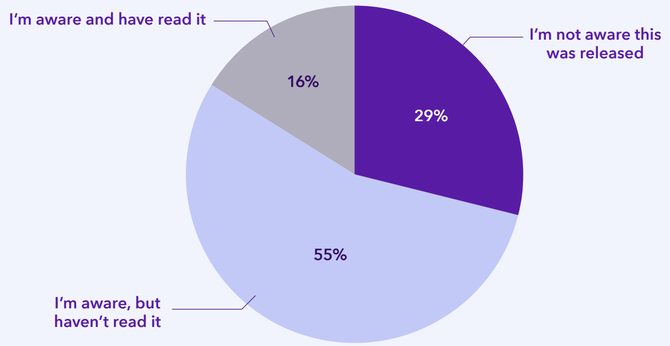
## Considerations for the new Government

Taxes, education and training, and cutting red tape are usually near the top of voter wish lists at election times. Our research also shows significant interest in a range of factors at the heart of our nation's resilience. A third of businesses want the government to establish clear and practical AI governance, 29% want more investment in infrastructure and a quarter want the national cyber-security capability strengthened.

*Confident performers* put even more weight on the importance of national cyber security capability, with 48% seeing this as a priority for the incoming government. They're less focused on the need for different tax settings to thrive, with just 38% mentioning this compared to 49% of all businesses although 45% want simplified regulations & compliance.

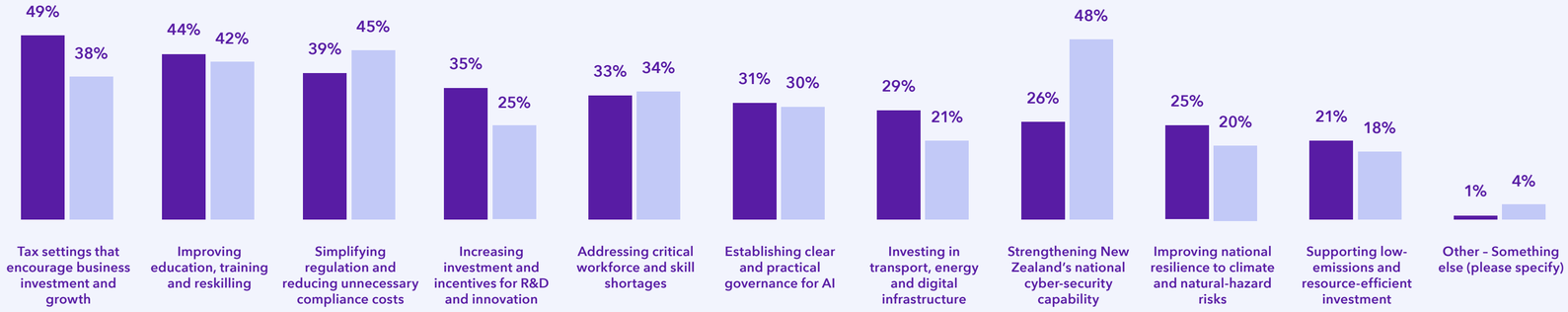
> *The new Cyber Security Strategy is an important signal that resilience, in particular cyber resilience, is now a national priority. But a strategy only works if people act on it, and most businesses haven't yet read it. Government, industry and business groups all have a part to play in turning it into practical guidance that businesses value and apply. In today's world, AI is both a tool to defend and a risk to resilience.*
>
> – **Karyn Pulley**, Network and Security Service Line Lead, Spark

## Most organisations haven't read NZ Cyber Security Strategy




Q The NZ government released the New Zealand Cyber Security Strategy 2026–2030 in February 2026. Which of these best represents your position?

## *Confident performers* ask Government to focus on cyber security capability




Q With 2026 being an election year what are the key things the future government should be focusing on to for the success of NZ Inc? (multiple selection)

All Businesses
Confident Performers

SECTION 2

# Resilience capability

Resilience should be seen as a strategic capability that protects performance, enables confident growth and strengthens the organisation's ability to adapt when necessary.

Disruption can come from anywhere: a cyber incident, a supplier outage, the loss of a key person or a sudden shift in the market. Resilience is about having the people, systems and controls to absorb disruption, recover quickly and come out of it stronger than before.

There are many business resilience frameworks.[3] This framework includes six pillars: financial, operational, technological, people and organisation, business model, and reputation.

> *In our experience, businesses tend to review their resilience after something has gone wrong, such as a network outage or cyber incident. Increasingly, the trigger is external. Insurers, regulators and customers want proof that critical systems, information and services are protected – and you need to get ahead of that. Investing in resilience before disruption hits means you recover faster, with less damage to customer confidence and revenue.*
>
> – **Sam Thumath**, GM Business Connectivity, Spark

**The 6 pillars of business resilience**

| Financial resilience | Operational resilience | Technology resilience | Organisational & people | Business model resilience | Reputational resilience |
|---|---|---|---|---|---|
| **Focus**<br>Cash buffers, capital efficiency, and liquidity. | **Focus**<br>Supply chain flexibility and production continuity. | **Focus**<br>Cyber security infrastructure scalability, backups. | **Focus**<br>Workforce agility, leadership depth, wellbeing. | **Focus**<br>Market adaptation and revenue diversification. | **Focus**<br>Stakeholder trust, brand equity, open communication. |
| **Key action**<br>Maintain runway, reduce debt, diversify cash flows. | **Key action**<br>Eliminate single points of dependency. | **Key action**<br>Simplify the IT stack, enforce rigorous access control. | **Key action**<br>Foster psychological safety and cross-train core skills. | **Key action**<br>Evolve value propositions to meet shifts in demand. | **Key action**<br>Maintain transparency with clients, employees, partners. |

# Technology

Technology now sits at the centre of how organisations operate, serve customers and grow. It links people, suppliers, information and the processes the business depends on. The deeper that dependency runs, the further a single disruption can spread. Yet technology is often treated as a utility, only noticed when it fails.

## Technology investment

We asked businesses where they'd invest if they had the money to grow their business. The most popular areas were workforce capability and skills (40%) and improving customer experience (34%). Leading-edge technology was on the list for fewer than one in four (24%) businesses, followed by improving cyber security at 19% and improving connectivity and network infrastructure at 18%.

## Cyber security investment

Some businesses are more focused on cyber security: 45% of *Confident performers* and 34% of large organisations (100 + FTE) would invest in it compared to 19% overall. Large organisations also expressed greater interest in investment in replacing legacy IT systems (25% v 17% of all businesses) and investing in leading-edge technology (32% v 23% of all businesses).

### Where businesses would invest to grow




Q Thinking now about your own business/the business you work in. If you had money for investing to grow the business which of the following areas would you spend it?

# Barriers to technology adoption

No one is expecting new technology to come easily, with a host of barriers complicating adoption. Large organisations (100+ FTEs) view most barriers as more challenging. This may reflect their size, or an underappreciation of potential difficulties among smaller organisations.




Q Which, if any of the following challenges are you facing for digital adoption in your business?

SECTION 3

# Resilience enablers

## Technology capabilites

New technologies, cloud adoption, automation and AI enable greater levels of resilience, productivity and growth. They also introduce new challenges. Layered on ageing platforms and accumulated technical debt, they can make the environment expensive to secure, harder to change and create greater levels of risk for disruption.

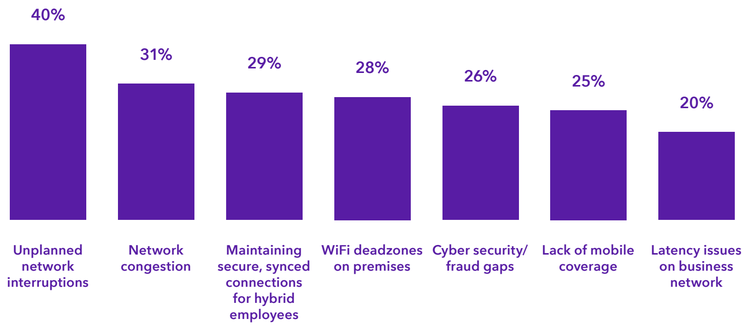
Resilience depends on a set of technology capabilities working together. This section looks at four of them: reliable networks that keep people and systems connected, cyber security that protects operations and trust, AI that supports productivity and adaptability, and well-managed data that enables insight, recovery and confident decision-making.

> *Some businesses think of connectivity like power or water: a utility you think about only when it stops working or performs poorly. Today, work happens anywhere and everywhere. Resilient businesses understand the risk and cost to their business if it is disrupted. We work with our customers to help them introduce new solutions that keep them always connected.*
>
> – **Stephanie Cunneen,** Business Mobile Service Line Lead, Spark

## Connectivity

Reliable connectivity is foundational to enabling a business to operate. Yet seven in 10 businesses haven't got all the basics right, with a range of issues compromising their connectivity. Among those with issues, unplanned network interruptions (40%) topped the list (47% 50–99 FTE firms), followed by network congestion (31%), maintaining synced connections for hybrid workers (29%, rising to 39% for organisations FTE 100+) and on-premises WiFi dead spots (28%).

Despite their frustrations, few businesses expressed any desire to invest in these areas. Just 18% said they'd invest in improving connectivity and network performance if given money to grow their business.




Q 'Are any of the following connectivity issues affecting your business' productivity and resilience? Choose all that apply (graph excludes those with no issues)

CASE STUDY

## Satellite broadband delivers where cables can't: Discover Waitomo

For businesses in areas prone to landslides or frequent excavation, a single-cut fibre cable can take everything offline. A resilient connection removes that single point of failure, and satellite broadband offers one that doesn't depend on what happens underground. Even so, many businesses are hesitant about satellite. Will it keep working in bad weather, under thick cloud cover? What about speeds? Can it cope with video? For Discover Waitomo, home to New Zealand's world-famous tourist attractions Waitomo Glowworm Caves, the Legendary Blackwater Rafting Co, and the iconic Waitomo Homestead, Spark's Starlink satellite offering has been rock-solid.

**Curse of the roadside excavator:** David Goldman, Discover Waitomo's IT Operations Manager, estimates that in his 12 years with the tourism operator, the Fibre link running alongside State Highway 3 – Waitomo's main visitor access route – has been severed 30 times. Mobile networks provided secondary options for data connections, but in the deep bush-clad expanse of the Waitomo district, coverage isn't ever a sure thing. Mobile networks provided secondary options for data connections, but in the deep bush-clad expanse of the Waitomo district, coverage is never a sure thing. And Goldman had experienced several instances when both internet and mobile networks failed simultaneously. The absence of a dependable fallback position made him nervous.

**Putting Starlink to the test:** Seeing the steep cost of running Fibre to Discover Waitomo's caving operations, Goldman decided to put Starlink to the test. Discover Waitomo installed a residential-grade Starlink connection at its Ruakuri Caves site, 5KM southwest of the main glowworm caves. With limited 4G coverage in the area, he saw it as a true test for satellite internet—and he was quickly impressed.

"You can barely make phone calls out there," Goldman said. "We installed a residential Starlink connection and ran it for a few months. It never went down – it just kept running, and as soon as Fibre went down a few more times, I was like, OK, let's give this a go."

**Going large:** Success at Ruakuri encouraged Goldman to run a proof-of-concept for a business-grade version of Starlink, which features a larger, higher-gain dish, at the Waitomo Homestead, a café, restaurant and gardens, with accommodation options.

Social media is perhaps the most powerful promotional lever for tourism operators, making visitor experiences more shareable. On this front Starlink might be the company's greatest marketing accessory, most evident at Discover Waitomo's blackwater rafting base and launch site, where excited tourists eagerly upload clips of their underground experience.

The frequent faults and slower speeds of onsite VDSL had made the process of supplying photos of the rafting experience to customers painfully slow. Starlink has been a massive boost, encouraging the firm to go 'cashless' at its blackwater rafting base – something they wouldn't have considered without reliably fast connectivity.

Learn more



# Cyber security

Cyber security is key to both business productivity and resilience. It helps businesses keep people, systems and data operating securely, reducing disruption and enabling employees to work with confidence. Strong security also allows businesses to adopt new technologies, including AI, while protecting customer trust and strengthening their ability to respond and recover when incidents occur.

## Cyber security incident

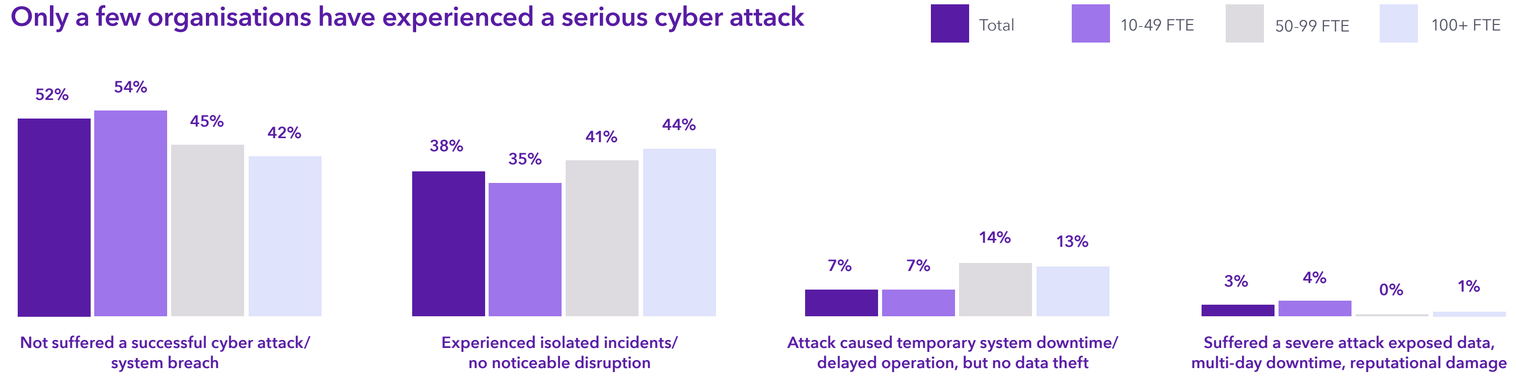
Our research shows that almost half (48%) of businesses surveyed have experienced a cyber security incident (58% among large businesses 100+ FTE). This finding is in line with the National Cyber Security Centre's (NCSC) SME Cyber Security Behaviour Tracker 2026, which found 53% of SMEs (0 to 50 FTE) had experienced a cyber threat or attack in the previous six months.[4]

Larger organisations (100+ FTEs) may be bigger targets for cyber criminals or suffer incidents that create more ripples. It's also possible that smaller organisations don't always recognise the signs.

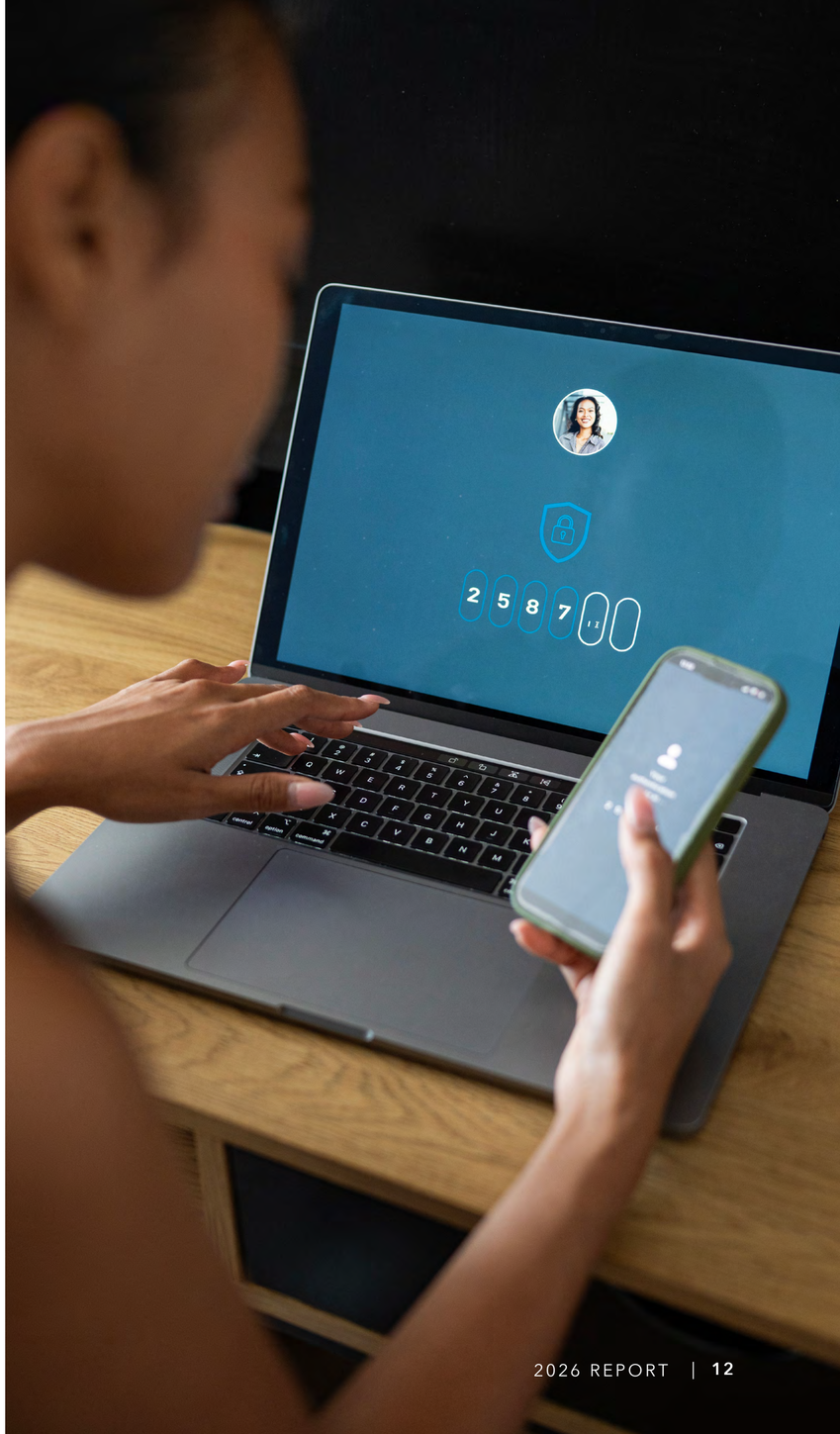
## Cyber incident impact

Overall, almost a third (29%) mentioned cyber security as a challenge currently having a significant impact on their organisation. So far, businesses appear to have got off lightly, with just 10% reporting to having experienced significant impacts stemming from a cyber security attack, including downtime or loss of data. The low impact so far may explain why so few (19%) see cyber security as a priority for further investment.

### Only a few organisations have experienced a serious cyber attack



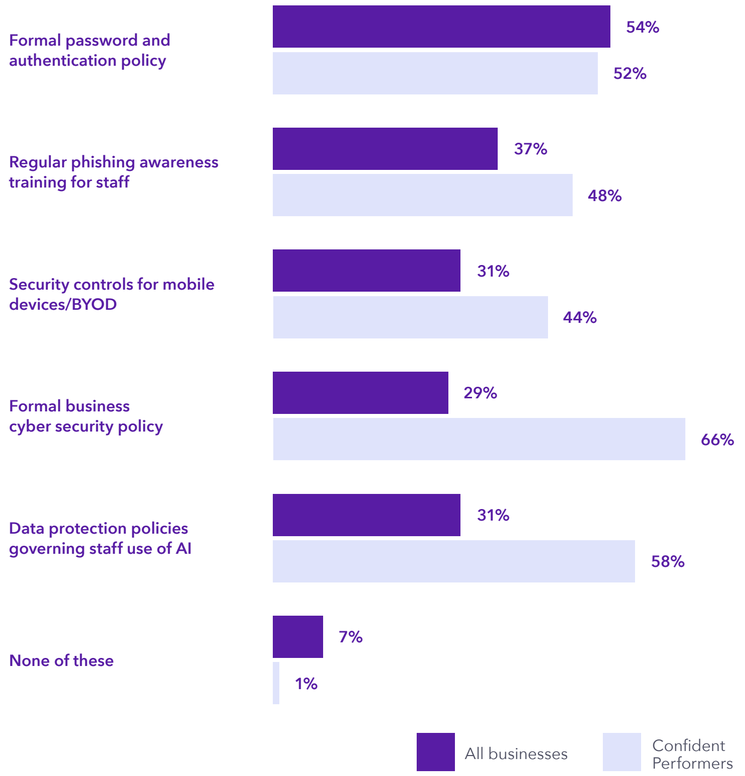

Q Which of the following best describes your organization's history of cyber security attacks (directly or through suppliers/partners) and their overall impact on the business within the past 12-24 months? (Please select the single highest level that applies to your organization.)



## Cyber security measures

Only 54% of all businesses have a formal password policy. There are fewer protections for popular workplace tools: only third have policies to govern the use of AI (31%) or apply security controls to mobile devices (31%).

### *Confident performers* have stronger cyber security measures




Q Which of the following cyber security measures does your business currently have in place?

*Confident performers* appear to take cyber security more seriously, with 66% having a formal business cyber security policy vs 29% overall. They're also significantly more likely to have policies that govern the use of AI (58% vs 31% of all businesses), offer phishing training (48% vs 37% of all businesses) and apply security controls to mobile/BYOD (44% vs 31%).

**Spark view: Cyber security**

*The fact that most businesses have come through a cyber incident without serious damage is good news, but it can also teach the wrong lesson. Every attack that doesn't do any harm makes it easier to believe the next one won't either. Often, what protected the business was luck, or an attacker who moved on to an easier target.*

*Resilient businesses treat a near-miss as a warning, understand what almost happened, close the gap and work on the assumption that at some point something will get through. It's about being proactive and that's where policies, tools and training will make a difference.*

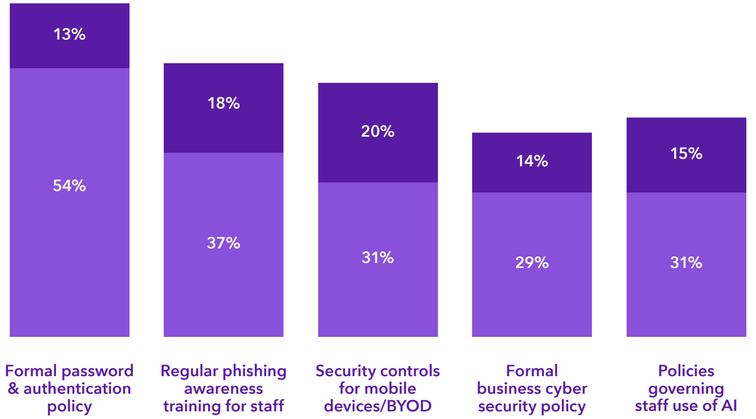
– **Mahadev Nanda**,
Head of Cyber Defence Operations, Spark

## Cyber security investment

They'd like to do more – nearly half would like to invest in improving their cyber security (45% vs 19%) and making a bigger play with leading-edge technology (45% vs 16% overall).

Few companies appear to be focused on improving their cyber security in the next 12 months. Just 14% plan to implement a cyber security policy in the next year. Added to the 29% who already have one, that still leaves more than half of businesses vulnerable. Similarly, only 46% of organisations currently have a policy governing staff use of AI or plan to implement one. On a positive note, 18% plan to introduce phishing training in the next year.

### Few organisations have or plan to implement a cyber security policy




Q Which of the following cyber security measures does your business currently have in place?

CASE STUDY

## Multi-year security programme strengthens Les Mills' cyber-defences

Les Mills NZ makes humans fit for life. Its world-class group fitness classes, including BodyPump®, RPM® and BodyCombat® are taught in 12 clubs across New Zealand. This reach depends on defendable technology. Working with Spark, Les Mills has strengthened its security posture to protect member information, maintain reliable club operations, and safeguard its member experience.

**Outmanoeuvring cyber-threats:** As cyber security threats grew more sophisticated, Les Mills NZ wanted specialist expertise to bolster its internal capability and long-term security position. It needed a partner that could assess where it stood, identify key risks, and set out a structured approach to greater resilience.

**Approach:** Spark began by assessing Les Mills' security controls, governance, policies, operational processes and overall maturity. The findings shaped a phased, multi-year roadmap covering governance and risk, security monitoring, incident response, identity and access management, data protection, vulnerability management and network security.

Spark worked alongside Les Mills' business and technology leaders so each security decision reflected business priorities and enterprise risk. That gave Les Mills the confidence to target its investments and keep momentum through the programme.

**Results and impact:** Les Mills now runs a coordinated, risk-based cyber security programme tied to its business objectives and enterprise risk framework. Priorities are clear, governance is stronger, and the business is far better placed to detect, respond to and recover from incidents as threats evolve. It also has a framework for prioritising security investment as its digital transformation continues.

"Working with Spark has helped us take a more structured, long-term approach to cyber security. We have a clearer understanding of our priorities, where to focus our investment, and how to keep strengthening our security, while still maintaining ownership of our overall strategy." – Mac Nathan, Head of Technology, Les Mills NZ

"Les Mills shows that cyber resilience isn't a product you buy – it's a capability you build, phase by phase. By pairing strategic planning with long-term execution, Les Mills has built a stronger foundation to adapt to disruption, manage cyber risk and embrace the opportunities of an increasingly AI-enabled world."
– Rameez A. Bhat, Principal Consultant Network and Security, Spark





CASE STUDY

## Failsafe connectivity for dynamic work environments: Port Nelson

Connectivity is easy to take for granted until it fails. In a busy warehouse, a dropped signal means scanners stop, records fall behind and workers lose the communications that keep them safe. Resilient operations need a network that holds up under pressure.

Port Nelson is a key gateway to the South Island, handling exports and imports including forestry products, pipfruit, wine and seafood. When a port like this slows down, the effects reach well beyond its own operations. For the port, unreliable WiFi had become a limit on how well it could run. With Spark's 5G+ Private Network, it has replaced patchy coverage with a dedicated network built for its operations, and laid the foundation it needs to adapt to whatever comes next.

**When WiFi isn't enough:** Dense warehouse environments left persistent gaps in WiFi coverage, and spending more didn't solve the problem. "No matter how much we invested in WiFi solutions, we couldn't get consistent performance," said Reagan Pattison, General Manager Business Transformation at Port Nelson. "Connectivity was becoming a real operational constraint for us."

**A network built for the site:** Spark worked with Ericsson to deploy a private 5G network covering around 30,000 square metres across three warehouses in Nelson and Blenheim, with a high-availability core at the port linked to small-cell radios inside the warehouses and across outdoor yards. Forklifts carry dual-SIM routers that switch to Spark's public 5G network when they move beyond the private coverage area. Staff can now scan pallets in real time, without interruption, as they move around the sites.

**Safer now, smarter later:** The network also supports a digital push-to-talk platform that improves real-time communications and provides location-based alerts. "Safety is fundamental in a port environment," Pattison said. Ericsson's NetCloud platform also gives the port better visibility of network performance, so teams can find and fix issues before they cause problems.

The network is also a platform for growth. It could support real-time asset tracking, predictive maintenance, enhanced CCTV, AI-enabled vision and automation.

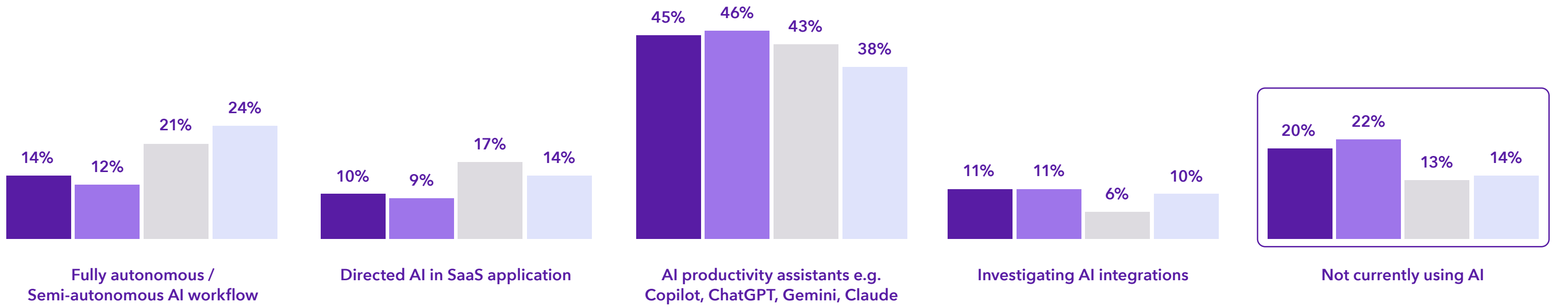
Learn more

# AI adoption

Most businesses (69%) use AI to some extent, with a further 11% either investing or considering AI integration. The sophistication is variable, with the bulk of businesses using desktop large language models (LLMs), such as ChatGPT and Claude (45%).

More sophisticated adoption remains in its infancy, with just 14% having fully or semi-autonomous AI workflows. Smaller organisations are less likely to be taking advantage of the new capabilities of AI, with just 14% using fully or semi-autonomous AI workflows, compared to 21% of businesses 50-99 FTE and 27% of the *Confident performers*.

## AI productivity assistants mostly commonly used AI




Q Which of the following best describes how the business is currently using AI? Choose all that apply

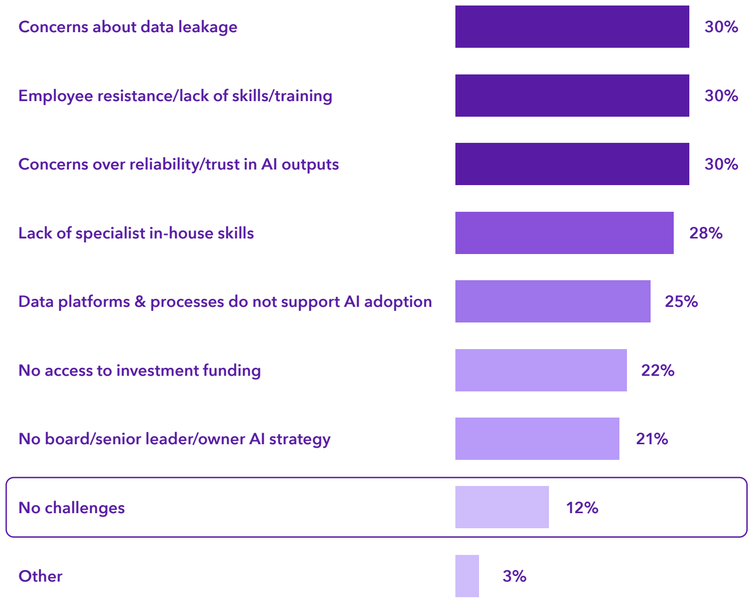
> *Businesses need to be on the leading side of the AI adoption curve to capture its productivity and growth opportunities. AI can make a business much more adaptable. It helps you spot changes sooner, respond faster and do more with the people you have.*
>
> *But achieving this requires deliberate investment to get on the front foot against any risk. It needs strong data foundations, the right skills and talent and clear data governance protocols. When these foundations are in place, organisations can move quickly without creating new exposures, whether that's sensitive data leaking out or a critical process relying on an unfamiliar tool.*
>
> – **Martin Norgrove**, Data and AI Service Line Lead, Spark



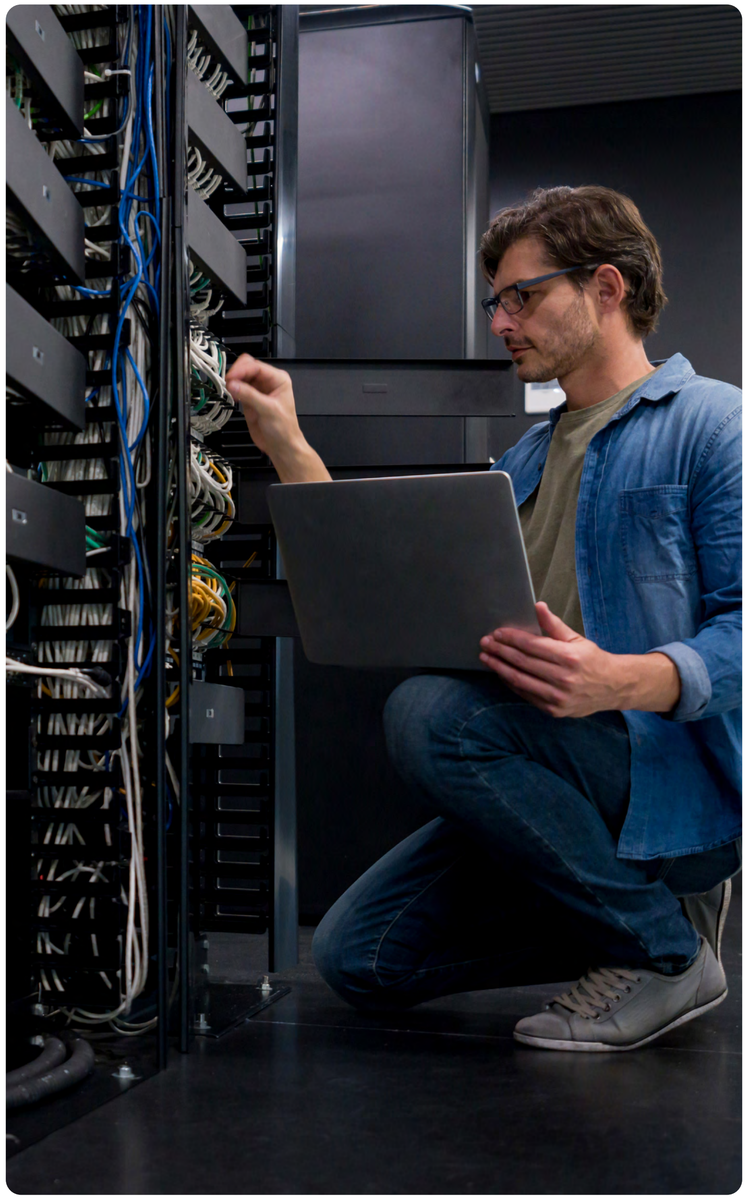
## Challenges adopting AI

Tentative AI adoption isn't surprising given the many barriers at play. Around three-in-ten organisations cite data leakage, employee resistance or skills deficits and concerns over trust and reliability of AI outputs. A lack of suitable in-house skills (30%) and incompatible platforms and processes (25%) are other issues. *Confident performers* are less concerned about data leakage (12% v 30% of all businesses) but say their main barrier is employee resistance or lack of skill/training (40% v 31% of all businesses).

### Businesses have multiple challenges to adopt AI




Q Which of the following challenges, if any, is your business facing with the further adoption of AI? (Choose all that apply)



## Data preparedness for AI Adoption

Data preparedness is arguably the most critical precondition for successful AI adoption, and yet most businesses surveyed are working with limited data integration. Advancing without the foundations in place is a big ask.

Around a quarter (26%) of businesses are working with siloed data, which is mainly used for reporting. Slightly more (33%) have at least aggregated data for dashboards and monitoring, with some exposure to AI tools. Just 21% of businesses have unified data and AI, embedding both in business processes to drive strategy and competitive advantage. More *Confident performers* are making much better use of their data, with just 6% having siloed data used only for reporting compared to 26% of all businesses.

### Majority of organisations have limited data integration

| | |
|---|---|
| Data and AI are core to business strategy and competitive advantage. Advanced AI is used at scale. | 4% |
| Data and AI are embedded in key business processes. Predictive AI models are widely used. | 17% |
| Data is integrated across teams. Analytics and AI models support specific decisions. | 20% |
| Data is brought together for dashboards and monitoring. Some standard AI or automation tools used. | 33% |
| Data is siloed in isolated tools. AI is not used. ***Confident performers* – 6%** | 26% |

Q Where would you rate your business data on the following scale for preparedness for adding AI?

CASE STUDY

## Building safety resilience with AI: Altus

A safe workplace is important not only for employees, but for the business itself:  without it, businesses face operational disruption and financial and reputational risk. Workplace rules are generally easy to follow. Over time, however, habits creep in, shortcuts are normalised and minor deviations become the way things are done.

In industrial environments like Altus® New Zealand (Altus), where forklifts, trucks and pedestrians share the same high-risk interaction zones, these drifting behaviours carry real risks. Resilient organisations catch the warning signs early, treating near-misses as data. While CCTV records what happens, AI Vision turns video footage into daily safety intelligence, flagging errant behaviours before they become incidents. Using Spark AI Vision, Altus has made that shift, and the results are already measurable.

**Managing risk in busy interaction zones:** There are many moving parts and safety challenges. George Green, the company's operations and system manager, has a special interest in software automation – in this case, how it can be used to improve health and safety. He identified forklift and vehicle movements as a key concern. "Sometimes people don't know they're doing anything wrong or putting themselves at risk," Green said.

**Turning CCTV into AI-powered safety intelligence:** Spark and its AI platform partner, Rush Digital, worked with Altus' existing IP-based security cameras operating at high-priority locations at the firm's Hamilton site: primarily high-risk interaction zones where forklifts, trucks and pedestrians often intersect.

Spark technicians installed a server onsite to handle local data capture and processing. The AI rules run on recorded footage from that server, flagging events and surfacing them via online dashboard reports.

**Up to 80% reduction in certain safety violations:** Altus' health and safety representative for Hamilton operations checks the AI Vision platform each morning, reviewing what was flagged from the previous day. Weekly and monthly trend reporting sits alongside the daily review, giving Altus both immediate visibility and a longer view on whether behaviours are improving. Though still in the early stages of full production, the results are already significant.

The deployment also carries weight under New Zealand's Health and Safety at Work Act, which requires businesses to take all reasonably practicable steps to keep workers safe. Green frames the AI vision system in those terms – not just as an operational tool, but as documented evidence of due diligence.

"The people in charge have got to show they've made every effort to keep their workers safe. So, everyone's very happy with what we're doing," he said.

Learn more



# Data storage

## Business critical data

To make the most of AI, businesses need their data to be in the right place: accessible when needed, securely stored and managed in a way that allows it to be connected and used effectively. Data storage decisions therefore shape not only resilience and recovery, but also how quickly and confidently an organisation can turn its data into insight, automation and better decisions.

Cloud has proven its value and is now the default operational foundation for many businesses. International cloud providers are the most common platform for business-critical data (45%), followed by on-premises infrastructure (31%), and local cloud providers (24%). Security, price and speed of access are big reasons why businesses chose to store their data in the cloud. Users of on-premises infrastructure tell a slightly different story – they're more likely than cloud users to cite wanting more control, access to decision makers and data sovereignty.

### Most businesses use international or local cloud operator

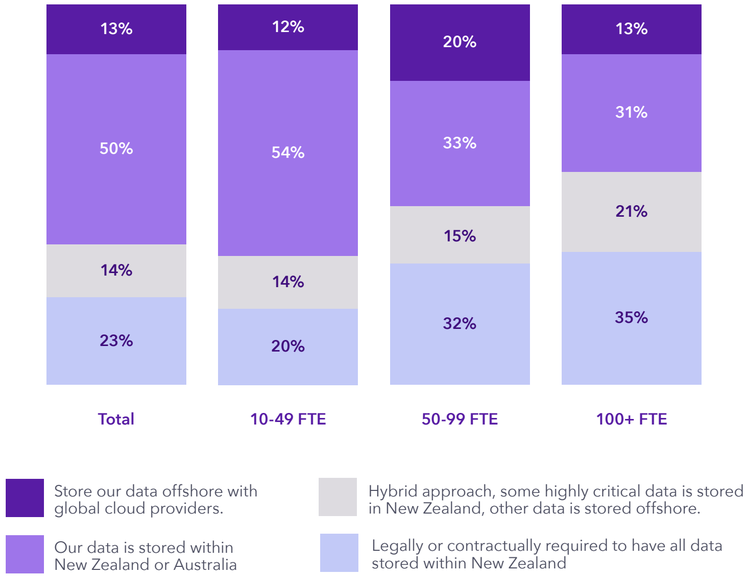



Q Which of the following best describes where your business mainly stores its business-critical data?

## Data policies

Data policies determine where data is held. A significant group of businesses (23%) say they are contractually required to store all data in New Zealand, rising to 35% of larger businesses. Most businesses have at least some data offshore, with half (50%) using New Zealand or Australian cloud services, and 14% using a hybrid approach of onshore and offshore storage.

### Most organisations store at least some data in New Zealand

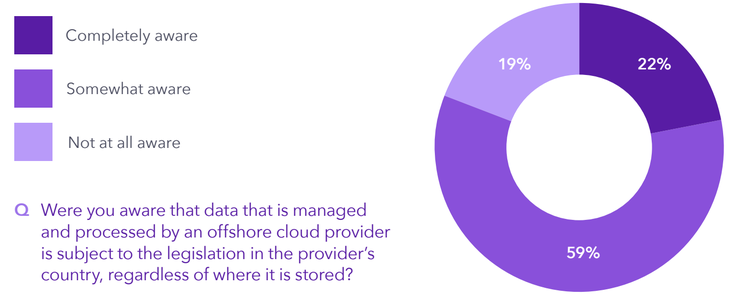



Q 'Some businesses believe it is important to manage which country their data resides in for data security and sovereignty reasons. Which of the following best describes your organisation's current data policy?

## Data sovereignty

Where data is stored, managed and processed determines the data sovereignty, that's which country's laws and regulatory requirements may apply to it. The graph below shows that only around one in five businesses (22%) were completely aware that data managed by an offshore provider is subject to the laws of that provider's country.

### Most are aware of data sovereignty implications




Q Were you aware that data that is managed and processed by an offshore cloud provider is subject to the legislation in the provider's country, regardless of where it is stored?

> *Data sovereignty is about understanding how the location and management of your data may affect the laws and regulatory requirements that apply to it. Using an offshore cloud provider may expose data to additional overseas laws or regulatory requirements, even where some data is stored in New Zealand. Understanding these implications is an important part of managing privacy, security and compliance risk.*
>
> – **Gregor White**, Cloud Service Line Lead, Spark

CASE STUDY

# Connectivity that keeps moving: H.W. Richardson Group

## Transport and logistics: Mobile and IoT connectivity

For a business that works on rural roads and back-country farms, mobile coverage maps don't tell the full story. Coverage is measured by where people live, and H.W. Richardson's trucks often work in more remote locations. Being resilient in that setting means knowing where mobile networks don't reach and using other technologies to cover any gaps. The diversified transport group, with more than 50 companies across New Zealand and Australia, has for over a decade relied on Spark to keep its people connected in the field. It has just signed a four-year renewal for 2,000-plus connected devices.

**A resilient office in every cab:** The company fitted around 500 of its trucks with roof-mounted cellular aerials, creating Wi-Fi-enabled cabs, run over Spark's Cisco IoT Control Center platform. Drivers also keep the hands-free radio handset they're used to, which now runs over mobile data. Telematics, electronic logbooks and job scheduling are fed back to dispatchers in real time, so drivers don't have to drive to the top of a hill to pick up their next job.

Real-time data also matters for safety. Electronic logbooks give dispatchers up-to-date information on drivers' work and rest periods, supporting H.W. Richardson's management of driver fatigue and safety.

**Data usage:** Spark listened and understood the importance of data usage to our business and the new contract was structured to meet our needs. "That opens up a whole new wave of innovations in the field – in IoT and other things," said Gareth Wishart, General Manager Technology and Innovation at H.W. Richardson Group, indicating future possibilities involving AI-based analysis and sending large volumes of data to the cloud for processing.

**Real world resilience:** The transport firm's many worksites run on fibre, with fallbacks, such as 4G, 5G and standby phones. "We don't want the Rolls-Royce or gold-plated solutions because you don't use these systems that often, but when you use them, they need to be reliable and user-friendly," Wishart said.

On that front, Wishart is looking to Spark to keep strengthening its network. "We look forward to continuing to work with Spark as connectivity technologies evolve." he said.

Next, H.W. Richardson is looking to work with Spark to explore the development of a regional hub for use in a disaster allowing local businesses to coordinate after a major event, such as an Alpine Fault rupture.



SECTION 4

# Resilience actions

*Resilience is a core business capability, enabling an organisation to keep serving customers, protect its people and data, adapt and keep investing in its future.*

*The right actions for improving resilience depend on your business's operating requirements, dependencies, risks and tolerance for disruption. Spark's team uses these three steps in consulting projects.*

*Resilient organisations adapt continuously, knowing that technology and secure connectivity is evolving. This isn't a one and done situation, it requires regular testing and a review of the organisation's operating environment. This is why many businesses find it helpful to engage external expertise to assess their current situation and develop a strategic roadmap.*

– **Chris Nicholson**
Enterprise Projects & Consulting Lead, Spark

### 1. Understand current state

Understanding your current position will highlight the right areas for investment. You can't prioritise investment until you know where you stand. Start with a clear picture of:

- Critical business services and the outcomes they support
- What customers and employees depend on
- The technology, applications, connectivity and data behind those services
- Key suppliers and third parties
- Cyber and operational exposure
- Technical debt and ageing systems
- Existing recovery capability
- How much disruption you can tolerate.

### 2. Build a roadmap

When developing your roadmap:

- Target the investments that make the biggest difference to business outcomes
- Separate immediate exposure from medium-term improvements and longer-term change
- Favour projects that strengthen resilience while simplifying and modernising your technology
- Match the plan to your budget, weighing what you can afford against what you can't afford not to do
- Set measures that track progress and make someone accountable.

### 3. Execute the roadmap

The roadmap contains sequenced initiatives designed to build your resilience capability. It should be a living document and include measures to test your resilience capability over time.

- Give each initiative a clear owner, and involve the right stakeholders
- Bring in a partner where you don't have the expertise in-house
- Review progress regularly, and revisit priorities when your risk picture changes. Only about a quarter of the businesses we surveyed have tested their resilience plans.

### Let's work together

Spark's team can help you assess your current business resilience capability, identify where to improve and put scalable solutions in place. Book a call with our team.

Contact us

# Endnotes

## Spark 2026 research study with New Zealand businesses

In August 2026, Spark commissioned Clemenger to research New Zealand businesses to understand the state of their technology foundations, their plans, where they invest, and how they manage risks ranging from cyber-attacks to variable connectivity.

- Online surveying included managers, directors and owners in organisations with 10+ employees.
- 404 responses categorised by business size: 10-49 n=150, 50-99 n=101, 100+ FTE=153
- For analysis purposes the data was weighted to reflect the distribution of NZ businesses with 10 or more employees.
- The research was completed between 21st August and 5th September 2026.

## References


1 In 2025, Spark produced a report *Lifting productivity: Moving New Zealand from getting by to getting ahead*. It was based on research commissioned through Clemenger Group with 397 business leaders surveyed from businesses 10+ employees. **https://www.spark.co.nz/online/large-business-govt/why-choose-spark/insights-reports/lifting-nz-productivity.html**

2 Cyber Security Strategy New Zealand's Cyber Security Strategy 2026–2030: **https://www.dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-2026-2030**

3 22316:2-18 The Foundations of Organizational Resilience is an international standard specifically designed to help organisations enhance resilience. There is also the Business Continuity Institute (BCI) Good Practice Guidelines.

4 **https://www.ncsc.govt.nz/assets/insights/Documents/2026-SME-Cyber-Security-Behaviour-Tracker.pdf**


UPLIFTING NETWORK RESILIENCE

## Spark Network

Reliable connectivity is critical during emergencies, when customers, communities and emergency services depend on telecommunications networks for essential communications. Natural disasters can place significant strain on network infrastructure, most commonly through loss of power or disruption to backhaul connections linking cell sites to the core network.

To manage these risks, Spark invests in a layered approach to resilience. Most cell sites are equipped with battery back-up and generator capability. In FY26, we were awarded a contract by National Infrastructure Funding and Financing (NIFF), in partnership with Connexa to strengthen the resilience of our mobile network by upgrading battery back-up at 295 cell towers across Aotearoa.

We also maintain satellite-connected emergency small cells that can be rapidly deployed when Fibre backhaul is compromised. We launched satellite-to-mobile services through Starlink to provide an additional connectivity option during disruptions. This service is available to customers on specific plans, however, in the event of a natural disaster, we open the service up to all Spark customers.

In parallel, we're rolling out AI-enhanced network monitoring to detect power loss, manage energy use and automatically prioritise essential services, such as calls and texts, to maintain critical communications in an emergency.

We also work closely with industry peers, government agencies and other infrastructure providers through the Telecommunications Forum (TCF) to support coordinated preparedness and response during major incidents.

# Ngā mihi