New Zealand Business Cyber Security Report 2026

MARCH 2026

10 YRS ANNIVERSARY EDITION

kordia®

Key Insights

Of the businesses we surveyed:

44%

Of large businesses were subjected to a cyber-attack or incident in the past 12 months

17%

Of cyber incidents resulted in personal information being accessed or stolen

ALMOST **1⁄6**

Incidents exploited AI misuse in their business

1 in 4

Say improper AI use is among their top 3 challenges to improving cyber security

61%

Of businesses impacted by a cyber incident suffered a serious business disruption

1 in 5

Impacted by a cyber incident faced financial extortion by cybercriminals

AI-powered cyber-attacks reached new levels in 2025. Is New Zealand prepared?

In 2025, digital transformation and Artificial Intelligence (AI) innovation continued to reshape how New Zealanders live, work, and trade. Yet this progress has been matched by the rapid evolution of cyber threats.

Globally, cybercriminals empowered by AI are attacking businesses at unprecedented speed. McKinsey reports that phishing volumes increased 1200% from 2022 to 2025, targeting an organisation every 39 seconds with a daily economic loss totalling $18 million.[1]

AI-driven tactics have dramatically improved the sophistication of attacks such as phishing, with studies showing that over 80% of phishing emails now contain AI-generated content that is far harder to distinguish from legitimate communications.

This surge in capability is compounded by a widening skills gap: only 14% of organisations have the right cyber talent, while the skills gap has grown by 8% since 2024, according to the World Economic Forum.[2]

These global trends are mirrored at home. According to the National Cyber Security Centre's Q3, 2025 Threat Report, New Zealand organisations suffered direct financial losses of NZ$12.4 million in Q3, a 118% increase compared to the previous quarter, and 110 incidents were triaged for specialist technical support because they were of potential national significance.[3] With our survey finding almost half of large businesses have suffered from a cyber incident in the past 12 months, the mandate is clear. Every New Zealand organisation must treat cyber security as a strategic priority, not a cost centre, to safeguard economic stability and societal trust in the digital age.

Who we spoke to..

Kordia commissioned independent research agency Perceptive to survey 247 business leaders from large New Zealand organisations (50 seats+) via an online survey, between 8 to 30 November, 2025.

Who we surveyed

General Manager	28%
Owner / Founder / CEO	16%
COO / Operations	14%
Managing Director	10%
CIO / CDO / CTO / IT Manager	9%
Director / Executive Director	8%
CFO / Finance Manager	8%
Security Leader	7%

Number of employees

50-99	31%
100-200	22%
201-500	18%
501+	29%

Location

Auckland	49%
Canterbury	14%
Wellington	12%
Rest of NZ	25%

Percentages rounded to nearest whole number.

Trends and threat landscape

Weaponisation of LLMs

In 2025, large language models (LLMs) were weaponised by attackers to radically increase the speed, scale and effectiveness of cyber operations. Microsoft's Digital Defence Report 2025 found that AI-assisted phishing campaigns achieved click-through rates of around 54%, compared with 12% for traditional phishing.

In a real-world example, Anthropic described multiple cases where Claude was used for semi-autonomous reconnaissance, social engineering and extortion. In one operation, 80–90% of activity was automated, reducing human effort to strategic oversight.

LLMs are lowering barriers to entry for cybercrime, enabling less sophisticated actors to conduct large-scale cyber campaigns with unprecedented efficiency.

Legislation seeks to assert national security posture

Governments are increasingly using cyber risk-focused legislation as a strategic lever to harden national security, economic resilience, and state authority.

A defining feature of this shift is the updating of critical infrastructure regulation, exemplified by the EU's NIS2 Directive, the UK's proposed Cyber Security and Resilience Bill, and Australia's SOCI Act. These broaden the scope of regulated entities, impose clearer accountability on boards, and grant regulators stronger enforcement and audit powers.

Governments are also using law to improve national cyber visibility and coordination, through mandatory incident and ransomware payment reporting (as seen in Australia), enabling faster state-led response.

Collectively, these laws reflect a strategic recalibration: cyber risk is no longer treated as an organisational IT issue, but as a matter of national resilience, sovereignty, and security.

> “ *Worldwide, new legislation is driving intelligence gathering and government empowerment, best practice is becoming regulation, and professional licensing is emerging. Business leaders should leverage cyber experts to lift their standards to international best practice, or risk being left behind.*
>
> **Patrick Sharp**
> **General Manager | Aura Information Security**

Trends and threat landscape

Malware-free attacks gain traction

The past year has seen threat actors increasingly favouring stealthier, malware-free intrusion techniques, with 'living off the land' (LOTL) attacks becoming dominant. These involve threat actors using legitimate, built-in systems and tools to carry out malicious activity, helping them blend in with normal operations and evade detection.

According to the CrowdStrike Global Threat Report 2025[4], more than 70% of observed intrusions were malware-free. Attackers are relying instead on legitimate administrative tools, stolen credentials, and hands-on-keyboard activity.

These techniques are popular because they are cheap, scalable, and difficult to attribute, blending seamlessly into normal IT activity. For organisations, this shift presents a profound challenge: traditional defences are ineffective and incident response is complicated by the absence of obvious malware indicators.

Exploitation at edge

Attacks targeting internet-facing infrastructure, such as VPN appliances, firewalls, and routers, rose sharply as attackers sought high-impact footholds outside traditional endpoints.

Verizon's 2025 Data Breach Investigations Report[5] found that exploitation of VPNs and other edge devices increased 8x compared to the prior year, shifting from involvement in around 3% of attack vectors to roughly 22% of exploit-based incidents. This highlights a strategic turn toward edge compromise as a primary entry point, with attackers leveraging such devices to gain network access without noisy malware.

Network scans and credential-stuffing campaigns operating from over 2.8 million unique IPs per day against VPNs, firewalls and gateways have been documented, illustrating the scale of opportunistic edge targeting.

AI becomes the attack surface

ChatGPT reached over 700 million weekly active users by mid-2025. It handles billions of messages per day, with about 30% of usage work-related, including drafting reports and coding assistance.

As AI tools became deeply integrated into workflows this year, often outside formal IT governance, the risk exposure of sensitive and commercial data increased dramatically.

One of the clearest examples was the DeepSeek AI exposure in early 2025. A misconfigured database leaked more than one million prompt and response records, including sensitive data, demonstrating how AI query logs can become a direct data-exfiltration avenue.

As businesses rapidly deploy AI tools without consistent governance and controls, AI platforms are increasingly attractive, scalable targets that materially expand the corporate attack surface.

Cyber-attacks & incidents

Nearly half of respondents told us their businesses suffered a cyber-attack or incident in the past 12 months. We asked those businesses to give us more information about the attack or incident and the impacts suffered as a result.

Almost half of businesses compromised

44% of businesses surveyed said they had suffered a successful cyber-attack in the past 12 months.

Social engineering proves effective

Attacks such as phishing, that successfully manipulate human behaviour, continue to be the dominant method for compromising businesses. 45% of attacks involved email phishing, text message phishing accounted for 14% of attacks and a further 6% involved voice or video deepfakes.

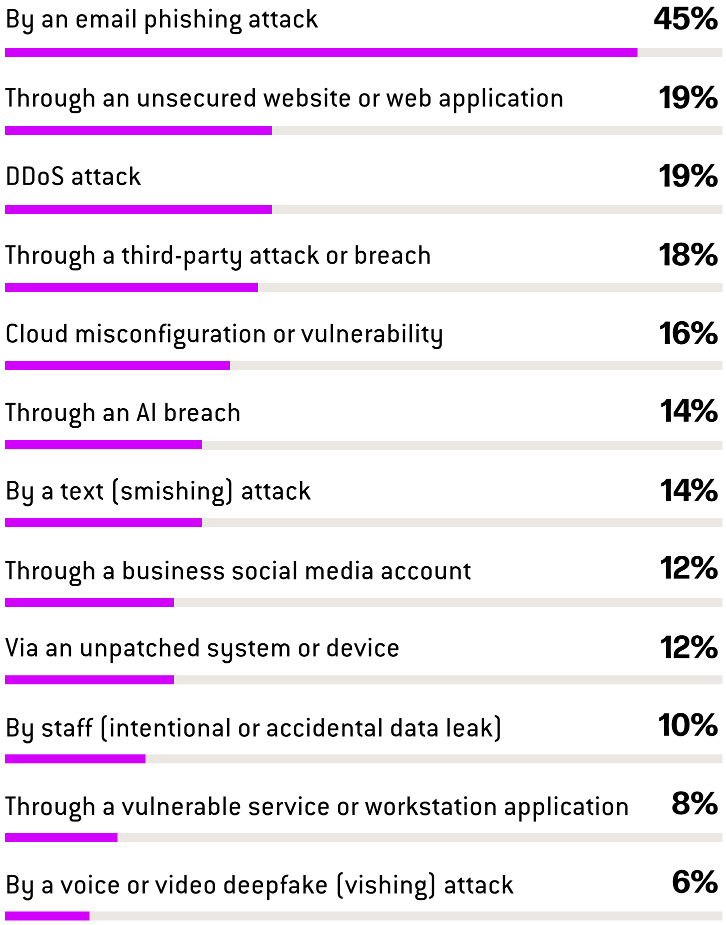
AI vulnerabilities emerge

Almost 1 in 6 attacks involved AI vulnerabilities or misuse, reflecting the risks associated with improper AI usage.

Vulnerable attack surfaces expose businesses

Almost 1 in 5 attacks were due to a vulnerable website or application, highlighting how attackers are looking opportunistically for weaknesses around internet facing devices.

How was your business compromised in the cyber-attack / incident?



By an email phishing attack	45%
Through an unsecured website or web application	19%
DDoS attack	19%
Through a third-party attack or breach	18%
Cloud misconfiguration or vulnerability	16%
Through an AI breach	14%
By a text (smishing) attack	14%
Through a business social media account	12%
Via an unpatched system or device	12%
By staff (intentional or accidental data leak)	10%
Through a vulnerable service or workstation application	8%
By a voice or video deepfake (vishing) attack	6%

Businesses were asked to select all responses that applied.

Consequences & impact

61% of attacks led to costly business impacts

From interrupted supply chains to fines and insurance claims, around two thirds of those who experienced a cyber incident reported some sort of impact on their business.

Financial extortion leaps up

The percentage of attacks featuring financial extortion lifted 5 percentage points year on year (19%, up from 14%), shifting into the top 3 impacts.

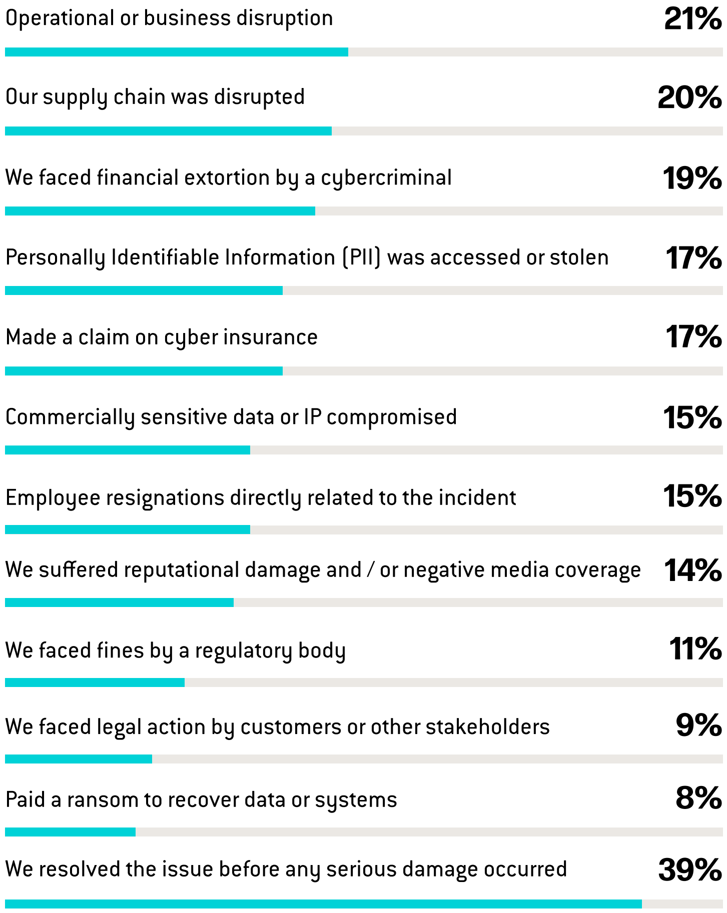
Sensitive information exposed

17% of attacks saw personal information exposed, while 15% involved the access or theft of commercially sensitive data.

Cybercrime pays

A small percentage (8%) of survey respondents admitted their businesses paid a ransom or extortion demand to a cybercriminal, highlighting gaps in resilience.

What was the impact of the cyber-attack or breach on your business?



Businesses were asked to select all responses that applied.

Lessons learned from cyber incidents

We asked New Zealand business leaders to tell us in their own words: "Based on learnings from your experiences during the cyber-attack or incident, what would you have done differently?"

Survey respondents who experienced a cyber incident indicate a broad range of learnings from their experience dealing with the attack. The most common theme that emerged from the survey respondents was improving or implementing employee training.

> *Better training for all of our internal staff so they are better equipped to know what is a phishing email and real.*

> *More education surrounding cyber-attacks.*

The second most important learning was is to invest in better security systems/policies.

> *Higher security and software for detection.*

> *We would have invested far more in cyber security systems.*

> *Ensure good practices for security are used when developing new features.*

The third most important learning was software updates/ preventative maintenance/ monitoring and scans.

> *Updated security software more often.*

> *More security checks to pick up possible hacks.*

> *I would have strengthened monitoring earlier and improved response coordination.*

The survey also revealed the toll that cyber-attacks are taking on New Zealand businesses, with comments on impacts:

> *We just really found it hard to get back on our feet after it.*

What keeps business leaders awake at night?

Employees accidentally exposing the business continues to be perceived as the biggest threat since reporting began, cited by just under half of respondents.

AI-generated cyber-attacks remain in the top three perceived threats, although the perceived risk has declined by 5 percentage points.

The second biggest threat viewed by business leaders was cyber-attacks leading to extortion. In a tough year for businesses with rising costs across the board, this is understandable.

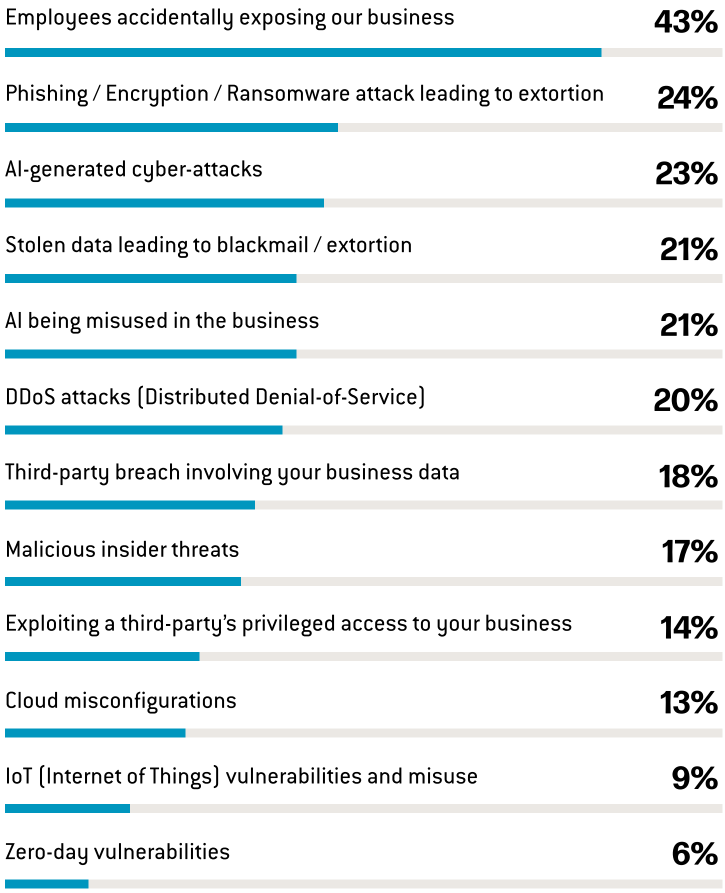
Threat perceptions vary by business size. Smaller organisations with 50-99 employees were most concerned about phishing and ransomware attacks leading to extortion.

For organisations with 100-200 employees, concern over AI misuse and malicious insider threats topped the concerns.

For businesses with 201-500 employees, the biggest perceived threat was Distributed Denial-of-Service (DDoS) attacks disrupting operations.

Finally, larger businesses with 500+ employees see AI-generated cyber-attacks as a major threat.

What do you perceive as the biggest threat to your business's cyber security posture?



Respondents were asked to pick their top 3.

Priorities and challenges

A lack of security awareness and good behaviours remains the top challenge for businesses for the third consecutive year.

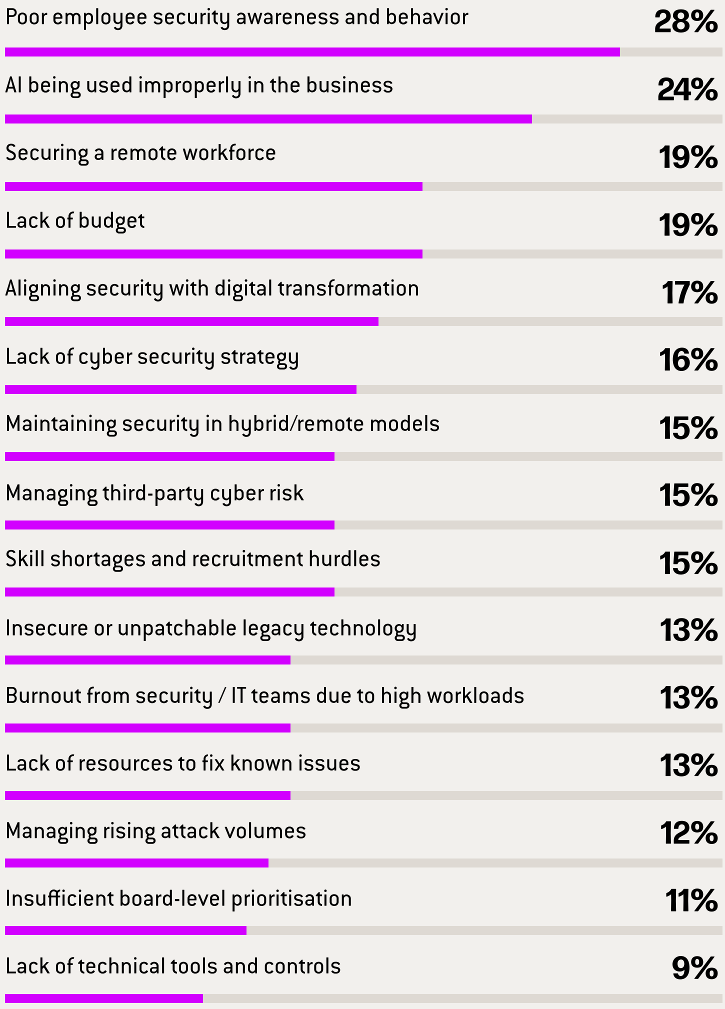
This is closely followed by AI being improperly used within the business, which has seen a significant increase from last year's survey (from 16% to 24%).

Respondents indicated a lack of budget has steadily risen over the past three surveys, as rising costs from vendors and a soft economic climate put cost pressure on technology and security budgets.

Managing third-party cyber risk, which was the second most cited challenge in 2024, has dropped to the middle of the list this year.

Perspective on top challenges varies depending on role. For General Managers and Directors/Executive Directors, the top challenge was the lack of cyber security awareness or good behaviours among employees. In contrast, Managing Directors and those in IT operational roles identify their biggest challenge as the improper use of AI within the business.

What are the top challenges to improving cyber security in the business you work in?



Respondents were asked to pick their top 3.

How cyber resilient are New Zealand's large businesses?

Of the businesses we surveyed:

⅓

Of cyber incidents took more than two months to resolve

30%

Lack confidence that they could recover from a major cyber-attack

1 in 3

Say they would be willing to pay a ransom to a cybercriminal

AROUND ¼

Do not have a comprehensive asset database

1 in 4

Have no cyber security awareness or training programme for their employees

AROUND ½

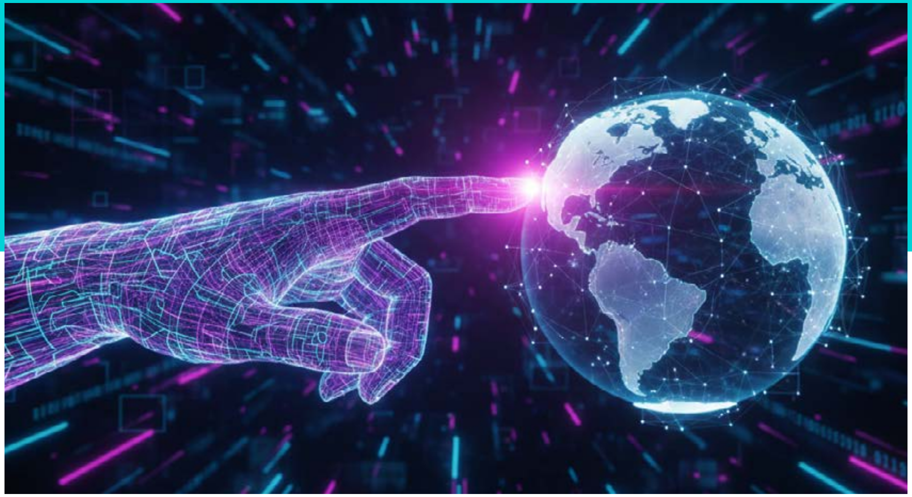
Have not practiced their incident response plans

AI and security risks

2025 saw a significant increase in concerns about AI being used improperly within the business, exposing new vulnerabilities and creating efficiencies for attackers.

While AI's productivity benefits have been lauded for enterprise use, and many of the big technology vendors have begun integrating LLM functionality into tools and platforms, New Zealand businesses continue to view AI as risky.

- 14% of businesses impacted by a cyber incident say they were compromised by an AI vulnerability.
- 1 in 4 businesses say AI-generated cyber-attacks are the biggest threat to their business.
- 24% of respondents say improper use of AI is a top challenge to improving cyber security.
- Two thirds of businesses say AI is perceived as an important risk area by their board of directors.



ANTHROPIC

Weaponising AI

In September 2025, AI company Anthropic detected a cybercrime campaign that it says represents the first large-scale attack largely executed by artificial intelligence rather than humans. The threat actor, thought to be a foreign state-sponsored group, manipulated Anthropic's Claude Code AI system, convincing it the tasks were legitimate cyber security testing. Claude then autonomously carried out most of the attack steps, including reconnaissance, vulnerability discovery, exploit development, credential harvesting, and data exfiltration, completing roughly 80–90% of the operation without human oversight. Around 30 global targets, including tech firms, financial institutions, chemical manufacturers, and government agencies, were probed, with a small number of successful intrusions. While Anthropic disrupted the campaign, the incident highlights how agentic AI systems can be misused for autonomous cyber-attacks.

Privacy and data breaches

New Zealand started 2026 with two major data breaches, at Manage My Health and Neighbourly, which drove intense media and public scrutiny. While 17% of New Zealand businesses saw a loss of personally identifiable information last year, these two cases were particularly notable as they were so public.

These breaches are a reminder that personal information continues to be highly sought-after by cybercriminals, given the financial incentives. Shadow AI – that is, unsanctioned use of AI by employees – has emerged as a significant factor in data breaches both overseas (Ponemon Institute Cost of Data Breach Report 2025) and in New Zealand, with 14% of all data breaches in New Zealand resulting from an AI vulnerability.

- 17% of businesses impacted by a cyber incident say personal information was stolen or accessed.
- 11% of businesses impacted by a cyber incident say they faced fines by a regulatory body.
- A data breach or confidential information leakage is the top concern cited by businesses when considering possible impacts from cyber-attacks and incidents.
- 15% of businesses impacted by a cyber incident say commercially sensitive data was breached.

How valuable are our data and credentials?

Attackers who breach businesses may sell data on the dark web to other threat actors for financial gain. Stolen data is most valuable when it is fresh, complete, rare, and sold by a trusted vendor, with a major price premium placed on credentials that can reliably bypass MFA. *(All figures below in USD.)*

"Fullz" (Complete identity packages)

A "fullz" package, containing a full name, address, Social Security Number (SSN), and date of birth, is typically priced between $20 and $100.

Identity documents

A scanned copy of a driver's license can range from $70 to $165. A passport scan might be listed for around $100.

Credit card (with CVV)

$10 - $40 (cards with >$5k limit can fetch ~$110 - $120)

Online bank login

$200 - $1,000+ (highly dependent on account balance)

Gmail account

~$60 - $65

Facebook account

~$45 - $50

Coinbase verified account

$120 - $250

Kraken verified account

Up to ~$1,170

Complete medical record

Up to $500+

Domain admin access

$35k +

Source: https://deepstrike.io/blog/dark-web-data-pricing-2025

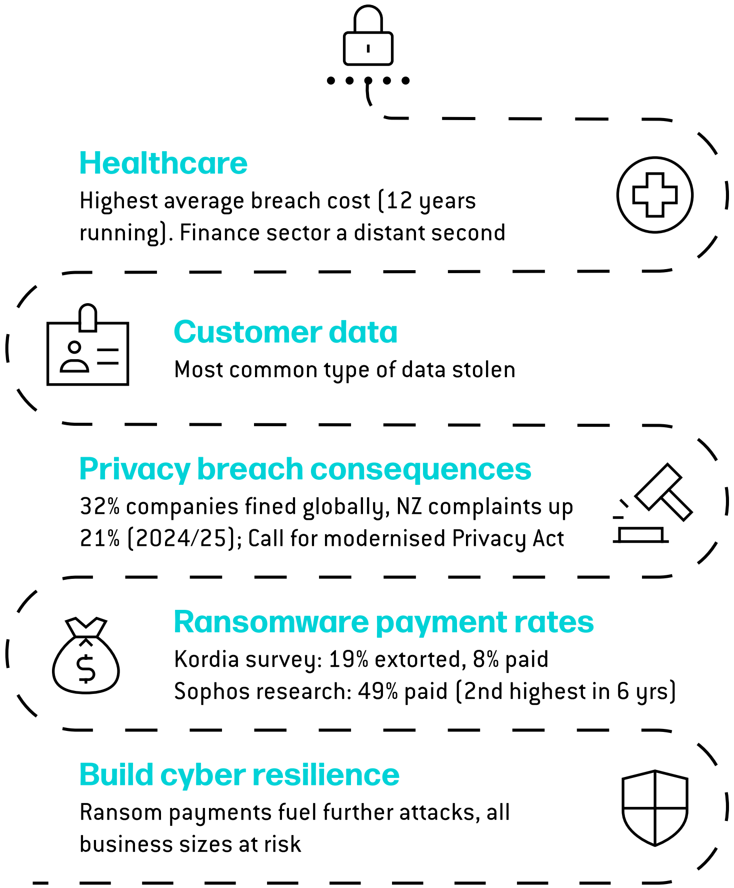
The cost of a breach

The Manage My Health breach brought the Healthcare sector into sharp focus - and New Zealand is not unique. Globally, and for the 12th consecutive year, Healthcare recorded the highest average breach cost, with the Finance sector a distant second (Ponemon Institute). Customer data was the most common type of data stolen.

Jurisdictions differ in how they approach consequences for privacy breaches. While 32% of companies around the world faced fines, New Zealand's Privacy Commissioner has noted the very high volumes of privacy complaints (an increase of 21% in 2024/25) in New Zealand, and called for modernisation of the Privacy Act 2020.

While 19% of businesses in Kordia's survey faced financial extortion and only 8% ended up paying, international research suggested a payment rate of 49% – the second highest payment rate in six years (Sophos State of Ransomware). Ransoms for data breaches are still a tool of choice for attackers, purely because they still work. But successful ransom payments will only fuel further activity, which is why it's crucial for businesses of all size to build their cyber resilience.

Cyber security breach trends & consequences



Healthcare
Highest average breach cost (12 years running). Finance sector a distant second

Customer data
Most common type of data stolen

Privacy breach consequences
32% companies fined globally, NZ complaints up 21% (2024/25); Call for modernised Privacy Act

Ransomware payment rates
Kordia survey: 19% extorted, 8% paid
Sophos research: 49% paid (2nd highest in 6 yrs)

Build cyber resilience
Ransom payments fuel further attacks, all business sizes at risk

The cost of a breach

Of the businesses we surveyed:

50%

Of Owners/CEOs say they would be willing to pay a ransom to a cybercriminal

8%

Of businesses impacted paid a ransom to a cybercriminal in the past year

1 in 5

Impacted by a cyber incident faced financial extortion by cybercriminals

1 in 5

Say stolen data leading to blackmail or extortion is their biggest threat

21%

Of businesses experienced major operational disruptions that halted daily work

17%

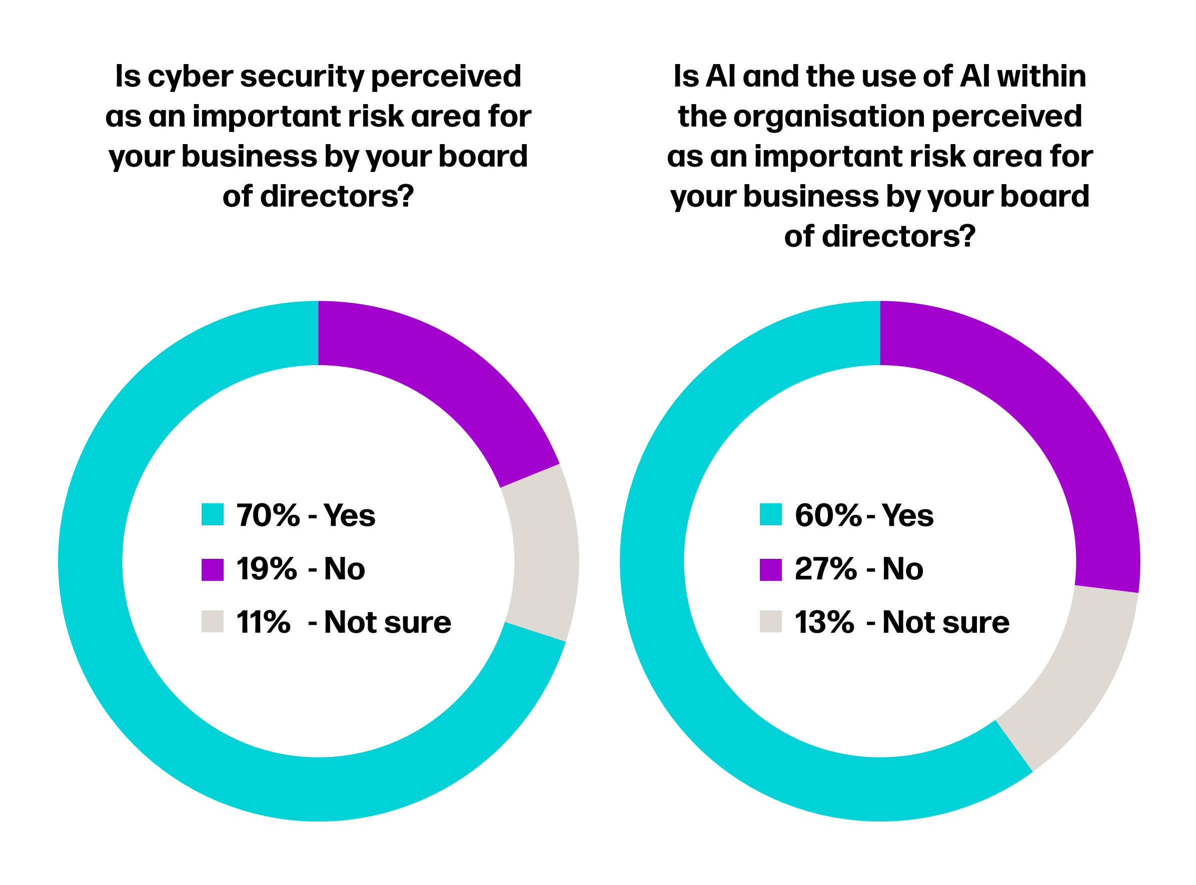
Had to make a formal claim on their cyber insurance following a breach

Cyber and the board

While most respondents indicated that their board regards cyber security as an important risk area, almost 20% of businesses do not. Those organisations that recognise the importance of cyber security have a more proactive approach to updating their understanding of cyber risks, whether continuously, scheduled, or triggered by service adoption or business change. In contrast, those who do not perceive cyber security as an important risk area are more likely to take an ad hoc approach to updates.

Half of all organisations' boards receive independent assurance of cyber resilience and readiness at least annually, with a further 21% (1 in 5) being updated every 2-3 years.

While private entities are more likely to treat AI & cyber risk as an operational IT matter, public sector organisations are the most likely to have integrated them and have them subject to independent testing and review.

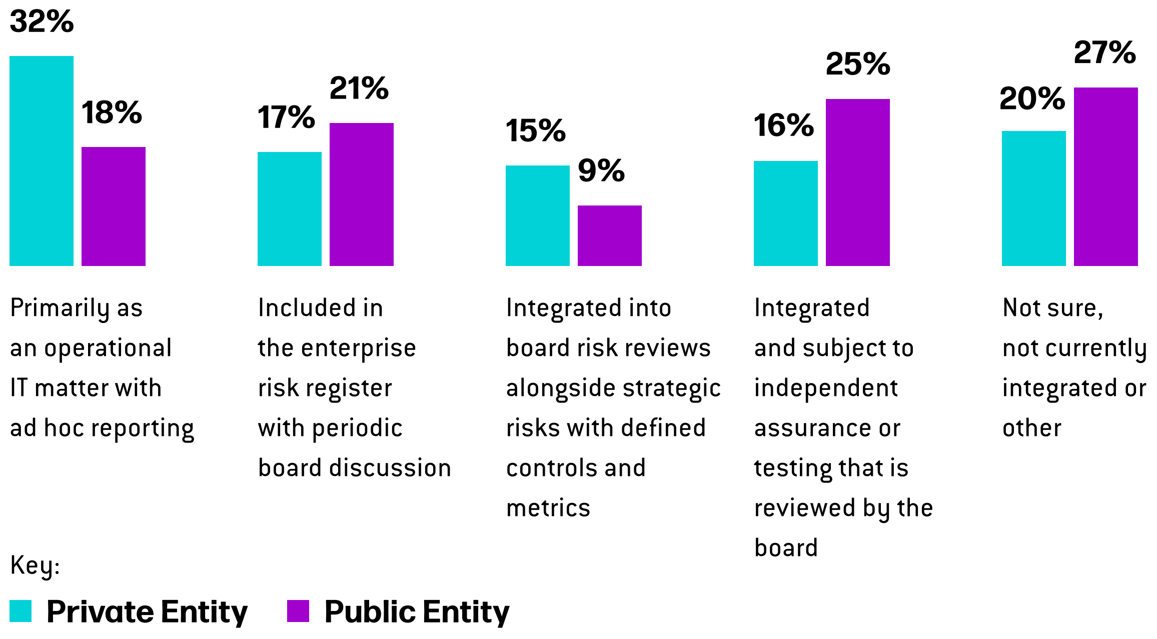


Is cyber security perceived as an important risk area for your business by your board of directors?

Is AI and the use of AI within the organisation perceived as an important risk area for your business by your board of directors?

Cyber and the board

How does your board integrate cyber risks from AI into enterprise risk and assurance?



Governance and legislation

The area of government support most requested by businesses remains education programmes to build awareness of cyber security best practice.

This year sees an increase in the proportion of survey respondents wanting harsher penalties for businesses that fail to protect data and those wanting mandatory reporting requirements for businesses impacted by major cyber security breaches.

To date, New Zealand's privacy laws have not been as punitive as other countries' when it comes to privacy breaches. For example, in New Zealand, penalties of up to NZ$10,000 are available for a small number of offences - compared to maximum penalties of more than AU$50m in Australia.

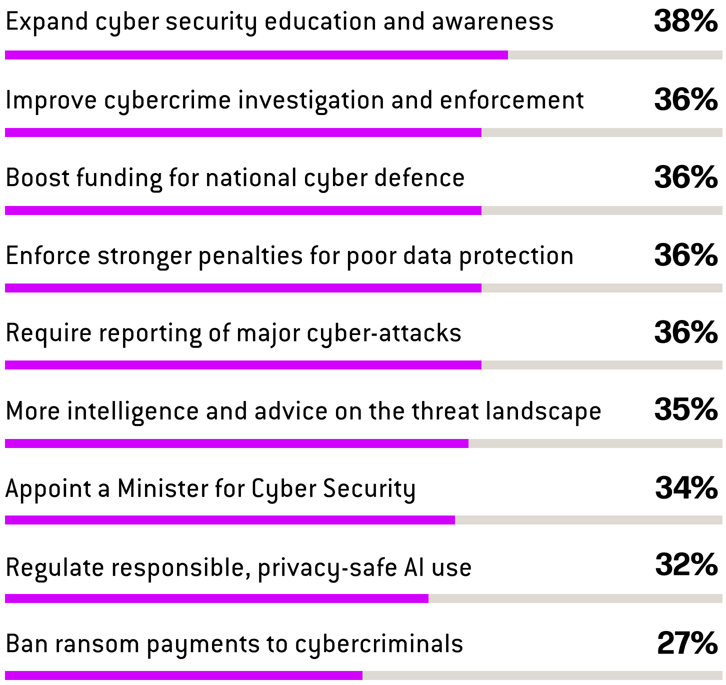
Cyber worldwide

Globally, cyber legislation has evolved from guidance to accountability and enforcement. The EU, UK and Australia are all explicitly tying cyber resilience to director accountability, expanding mandatory incident reporting, and moving from voluntary guidance to enforceable standards.

The process of professionalising the cyber industry is continuing, driving higher expectations of competence amongst security professionals.

These are decisive moves to unify government and business standards to defend against the scourge of state and criminal threat actors assaulting their countries.

What would you like the New Zealand Government to do to support cyber security for businesses in NZ?



Businesses were asked to select all responses that applied.

Four focus areas for businesses in 2026

1 Securing identity key

Cloud services, remote work, and edge devices have dissolved traditional network boundaries, leading attackers to increasingly target identities rather than infrastructure.

AI has further shifted the balance; social engineering is now highly targeted and uses voice and video media in addition to email. Once inside, weak identity controls allow attackers to take advantage of rapid privilege escalation and access to critical systems.

- Strong identity security can significantly reduce risk by preventing account takeover, constraining lateral movement, and limiting damage when breaches occur.
- Approaches such as phishing-resistant MFA, least-privilege access, and continuous identity verification directly disrupt modern attack chains.
- Identity-centric architectures like Zero Trust Network Access (ZTNA) and Secure Access Service Edge (SASE) ensure access is granted based on user, device, and context — not network location.

As we look toward 2026, prioritising strong, adaptive identity measures should be a priority for New Zealand organisations seeking resilience in today's threat landscape.

2 Complementary controls and continuous detection

Zero-day threats targeting common software components result in high volumes of impactful attacks.

- Understand the type of threat faced by each asset and select complementary controls to detect and protect.
- The speed at which vulnerabilities are being exploited has rapidly increased, and continuous detect and respond is needed.
- Layered security domains enable risk-aware defence in depth.

> “ *Most attackers don't hack in, they log on.*
>
> **Patrick Sharp**
> **General Manager | Aura Information Security**

Four focus areas for businesses in 2026

3 Elevate cyber risk accountability and make informed choices

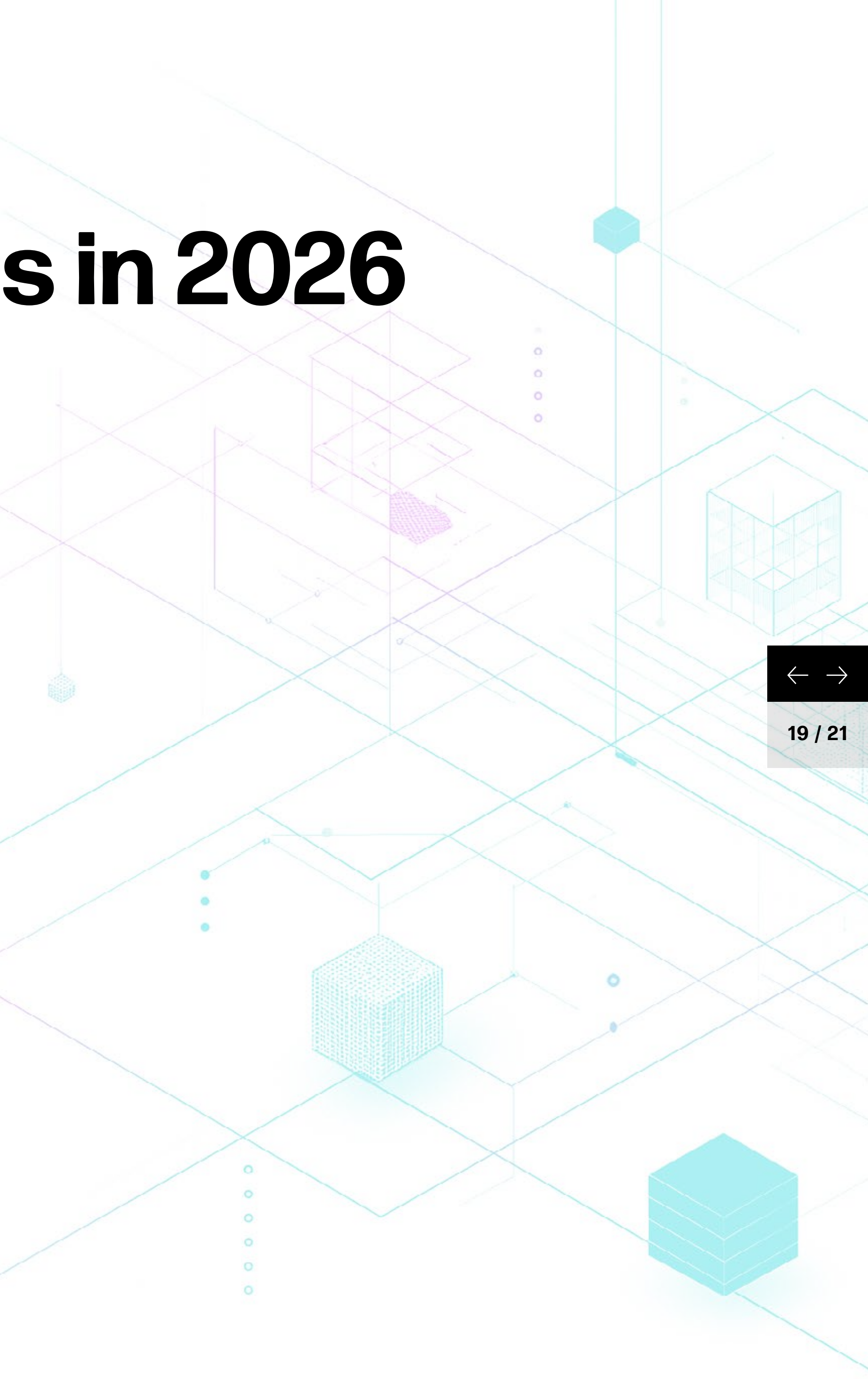
Globally, directors and executives are being held accountable for cyber resilience by shareholders and legislation.

- Cyber incidents can impact business operations, trust and reputation, and cost real money.
- Stakeholders recognise cyber resilience comes from risk-awareness, professional decision making and maintaining control effectiveness, and expect officers to manage their risk posture.
- A growing global drive for professionalism recognises that cyber security is complex and highly specialised. Make sure you are getting qualified advice and have set clear expectations of suppliers.

4 Upskill your people for an AI-first world

The use of AI further exacerbates common cyber security risks. It is essential to raise awareness and implement controls to avoid costly incidents.

- Review security training to reflect the current targeted use of vishing and deepfakes.
- Set guidelines with staff about AI use. Create an AI use policy and empower change through agile process rather than shadow AI.
- Ensure your Software Development Life Cycle (SDLC) and Software Bill of Materials (SBOM) processes are updated to reflect AI use in coding.
- Ensure data classification is well established and effectively enforced before introducing AI access.
- Understand how third parties are using AI tools to access your dataset and ensure security is in your control.



← →

Related resources

Managing third-party cyber risk

Discover the five areas you need to focus on when assessing third-party risk.

AI Policy checklist

An AI Usage Policy can help safeguard your business from data privacy risks. Get started with our guide.

Cyber Report 2025

Compare our latest findings with research conducted with New Zealand businesses in 2025.

Executive Incident Response checklist

This checklist can be used as a tool to help your organisation refine its incident response plan.

RANSOMWARE
A PRACTICAL GUIDE TO NAVIGATING RANSOMWARE RISKS AND PROTECTING YOUR BUSINESS
kordia

Ransomware Guide

Our Ransomware guide gives NZ business leaders the decision-making framework you need before an attack strikes.

Cyber Smart Hub

Visit our Cyber Smart Hub for tips and resources to help your business stay protected.

References

1. 5 must-read cybersecurity stories of 2025 | World Economic Forum 2. WEF_Global_Cybersecurity_Outlook_2025.pdf 3. NCSC report for Quarter 3 2025 shows large increase in reported financial losses 4. Crowdstrike global threat report 2025 5. Verizons 2025 Data Breach Investigations report

kordia®

KORDIA.CO.NZ