National Cyber Security Centre

Cyber Threat Report 2026

Pūrongo Tuma ā-Ipurangi 2026

An analysis report by the National Cyber Security Centre

Te Tira Tiaki
Government Communications Security Bureau

www.ncsc.govt.nz

Contents
Ngā kaupapa

Foreword
Whakapuakitanga

The cyber threat landscape is changing faster than ever

He tino tere rawa atu te hurihuri o te ao whakatuma ipurangi

Prepare now for the impact of AI

The 2026 Cyber Threat Report is being published at a time of particular volatility and disruption in the global environment.

New Zealand businesses and organisations are operating in a more fragmented global and regional security landscape, impacted by shifting power balances and ongoing conflicts.

Disruption isn't new. But now, to well-known factors such as geo-strategic competition and economic rivalry, we can add a powerful new disruptor: the deployment of frontier AI tools, with the challenges and opportunities they bring.

Leaders are responsible for cyber security

This report provides the National Cyber Security Centre's (NCSC) assessment of the key cyber security risks and threats facing New Zealand businesses and organisations. It is intended primarily for New Zealand leaders and decision makers, but it will also be relevant to anyone interested in cyber security. As you read, I encourage you to consider the potential implications of these threats for your organisation or business.

While frontier AI features strongly in this year's report, so do the familiar threats posed by cybercriminals, state actors, and issues around supply chains and social engineering.

My message to leaders is that cyber security needs your attention now more than ever. Based on the harm and impact that the NCSC is seeing, many New Zealand businesses and organisations could do better.

Government cannot protect your business or organisation from all the cyber threats identified in this report; that is your job. You are best placed to decide on the investments you make and how your staff and teams manage security. At the NCSC, we want to help you make informed decisions based on reliable threat information. This report aims to strengthen your understanding of the cyber threat environment and support efforts to improve your cyber security.

• • •

'My message to leaders is that cyber security needs your attention now more than ever.'

Advanced AI is here

Frontier AI models, the most advanced artificial intelligence systems, are putting reasoning and analytical capabilities previously accessible only to advanced nation states and the largest organisations, into the hands of individuals and groups. These models are supercharging existing trends in the global environment, with impacts that can be seen everywhere from the battlefield to the boardroom, and from global stock markets to the search engine on your mobile phone.

While the broader impacts of frontier AI are unpredictable, in the cyber security area we know it will enable faster identification of zero-day vulnerabilities, accelerate the reconnaissance of systems, automate brute force attacks and enhance the creation of phishing scams and deep-fakes.

At the NCSC we are focusing our efforts on understanding how these frontier AI models can support cyber defence, and developing actionable advice for New Zealand businesses, organisations and government about how to protect sensitive information and systems from malicious cyber actors.

Meanwhile leaders should be asking if their business or organisation is prepared for the impact of frontier AI on cyber security. Do you have the systems, processes and resources to patch systems more often, respond to vulnerabilities and breaches, and keep your people and their information safe and secure? If you are thinking about adopting AI tools for business purposes or to enhance cyber security, have you considered how to do this safely and responsibly?

State actors and cybercriminals are active in New Zealand

Much of this report focuses on the impact of AI now and into the future. But we must remember that state actors and cybercriminals are already causing significant harm to individuals, businesses and organisations. The number of reported incidents we classify as potentially of national significance increased last year, with an 18% increase in criminal or financially motivated incidents.

We expect New Zealand businesses, organisations and individuals will continue to face a significant volume of malicious cyber activity driven by challenges to global norms of responsible state behaviour, overseas conflict and rapid changes in technology. State actors and cybercriminals are rapidly adapting their tools and techniques, taking advantage of AI to deliver cyber threats at greater speed and scale using automated attacks, customised social engineering techniques, and exploitation of personal information and credentials.

Preparation is more important than ever

The NCSC's assessment is that the threats described in this report are here, now, and represent a tangible risk of business disruption. Given the transformational effect of new technologies, there may be little warning of disruption before it happens, and some threats may not be preventable. If you think it can't happen to you, you're wrong.

This reshaping of the threat environment demands the attention of leaders including Boards, CEOs and CIOs. Organisations should prepare for cyber disruption, and you need to start making changes at a governance and operational level to be better prepared.

Fortunately, there are real, practical actions that organisations and businesses of all sizes and capabilities can put in place to defend your systems from cyber threat. Information about these actions is included in this report, together with guidance about the big issues which we believe leaders should be focusing on.

Too many New Zealand organisations still aren't doing the basics of cyber security right. This is our greatest challenge and our greatest opportunity. The good news is we know what we need to do, and that taking action will protect you against last year's human and this year's AI-enabled threats.

Catriona Robinson
Deputy Director-General
National Cyber Security Centre

About us
He kupu mō mātou

The National Cyber Security Centre (NCSC) is part of the Government Communications Security Bureau, or GCSB. Our role is to make it easy for everyone in New Zealand to play their part in keeping the country cyber secure. We deliver our work through three primary approaches:

1. We support all New Zealanders to act on informed information.
2. We work with key players to build good cyber security basics into New Zealand's cyber ecosystem and essential services.
3. We use our mandate, relationships and specialist capabilities to counter the most serious harms.

The Cyber Threat Report is the NCSC's annual independent assessment of the cyber threat environment facing New Zealand organisations, businesses and individuals. It should not be considered a government policy document.

Getting in touch
Whakapā mai

Visit **ncsc.govt.nz** for more cyber security advice, and information about NCSC programmes. On our website you can:

- Report a cyber security incident
- Subscribe to receive NCSC news and updates
- Subscribe to receive alerts about current cyber security threats and vulnerabilities, and how to mitigate their impact.

General enquiries

For all general enquiries, email us at **info@ncsc.govt.nz**

Follow the NCSC on LinkedIn. **www.linkedin.com/company/ncsc-nz**

Individuals and small businesses

For cyber security advice aimed at everyday New Zealanders and small businesses, visit Own Your Online at **ownyouronline.govt.nz**

www.facebook.com/ownyouronline

www.instagram.com/ownyouronline/

www.youtube.com/@OwnYourOnline

www.linkedin.com/company/ownyouronline

Key judgements 2026
Ngā Whakataunga matua mō te tau 2026

Cyber security is a critically important consideration for all New Zealand organisations.

This report sets out five judgements for 2026 regarding cyber security. Each judgement describes a key aspect of the current threat landscape that we think is relevant for leaders and decision makers.

The judgements are:

1. Artificial Intelligence is rapidly reshaping the cyber landscape: Frontier AI will supercharge the risks and opportunities
2. State-sponsored cyber activity is a persistent threat to New Zealand organisations and businesses
3. Cybercrime and extortion are escalating in severity
4. You can't defend what you don't know. Digital supply chains continue to be a major risk for New Zealand businesses
5. Social engineering is a persistent threat to organisations and businesses

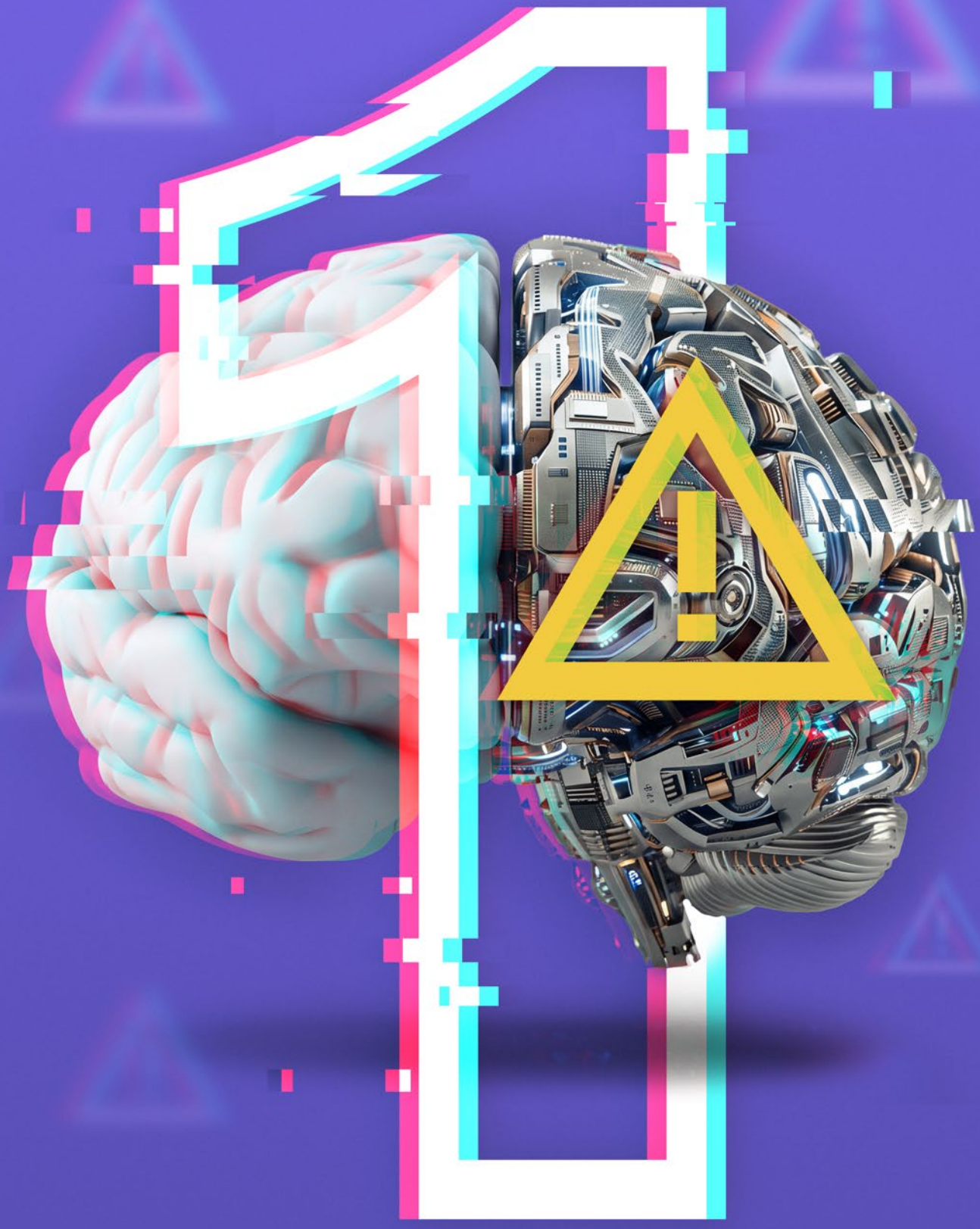
Our judgements are based on our work both domestically and internationally. This is not an exhaustive list, but they include some of the most prominent, noteworthy and recurrent issues that we observe.

These judgements also reflect the trends in the more severe incidents the NCSC responded to this year. Of the 4673 reports received by the NCSC during the 2025/26 financial year, 369 incidents were triaged as incidents of potential national significance, meaning they received additional analysis and support. Four incidents were classified as C2 or highly significant.

The statistics and case studies used throughout the report are primarily based on our work between 1 July 2025 and 30 June 2026. We recognise that we do not have perfect understanding of the New Zealand cyber security environment, so these should be regarded as illustrative rather than a complete overview.

This report will give you a picture of how the cyber security environment is evolving and how these changes should be factored into your risk assessments and strategic thinking.

We hope this information will help you consider how well your organisation is prepared for the current cyber threat landscape and will help to inform the cyber security investment and resourcing decisions you make in your organisation. This information should be considered alongside other sources of information that inform your cyber security decisions.



Artificial Intelligence is rapidly reshaping the cyber landscape. Frontier AI will supercharge the risks and opportunities

He tere hoki te huri a te Atamai Hangahanga (AI) i te ao ipurangi: He kaha te whakaara a Frontier AI i ngā mōrea me ngā arawātea

Artificial Intelligence (AI) continues to rapidly reshape the cyber landscape. AI capabilities are already in the hands of malicious actors and are being used to enhance the speed and scale of cyber attacks, create deep-fakes, execute targeted phishing attacks, and undertake reconnaissance at scale.

The insight we have is that frontier AI models provide a step-change in capability beyond existing AI tools, including the ability to identify zero-day vulnerabilities and automate attacks that currently require human control.

The NCSC believes that the trajectory of AI development is such that, by early 2027, malicious actors may have access to advanced AI capabilities currently available only through leading frontier AI models. The threat to businesses and organisations is real. There will be incidents and disruptions, potentially with little warning. The time to prepare your defences is now.

Why does this matter?

For some time, AI models have enabled cybercrime, espionage and other malicious online activity. Now, the deployment of frontier AI systems will lead to a step-change in capabilities, both positive and negative. While frontier AI models can and in some circumstances already are being used to improve cyber defences, it is certain they will be used by cybercriminals and state actors for malicious purposes.

The key capability shifts to be aware of include:

Zero-day vulnerabilities. Frontier AI can better analyse code to identify vulnerabilities, and AI agents are becoming capable of chaining together vulnerabilities into more complex exploits. On the other hand, the same tools can be used by defenders to strengthen code, identify exploitable weaknesses in system configuration, or respond to security events at speed.

Reconnaissance. Frontier AI can automate and dramatically accelerate reconnaissance by malicious actors of your business, its people and systems. This capability can be used to develop personalised attacks on individuals and identify weaknesses in your systems.

Brute forcing. Brute force attacks use compute power and automation to guess username and password credentials in order to access a system or tool. AI makes brute forcing smarter and faster. It also enables the fusion of information gained from multiple sources (e.g. social media and stolen credentials) to generate highly targeted attacks.

Personalised phishing and deep fakes. AI is enabling the easier creation of customised messages from what appear to be trusted sources. These messages are moving beyond text-based messages to convincing and personalised audio and video content. This capability is enhanced by AI translation tools that allow cybercriminals to target individuals across many communities and cultures with messages in their own languages that appear authentic.

The time to act is now. Cyber defence fundamentals are essential.

Highly capable AI models are already widely available and already being used by malicious actors. Our message is that you should act now to apply basic cyber security principles to your systems and support your people to apply good cyber behaviours.

The best defence against cyber attacks, by humans or AI, continues to be effective cyber security controls. What has changed is the urgency and resourcing to deliver and maintain these controls. We recommend that organisations review their current cyber security controls to ensure they are fit-for-purpose and sufficiently resourced. The National Cyber Security Centre (NCSC) has published guidance for cyber defenders and business leaders to help them understand the risk of AI-enabled attacks.

- **Reduce your attack surface:** Limit unnecessary system access and external connectivity. Challenge whether systems need to be exposed at all and isolate those that do not.
- **Accelerate patching processes:** AI is shortening the time between vulnerability discovery and exploitation. Delays in patching increase risk, especially for operational systems with long update cycles. Prioritise security updates to manage risks.
- **Address legacy systems:** Unsupported systems are easy targets. They don't just represent technical debt, they are strategic liabilities. Ensure assets nearing the end of their supportable life are replaced.
- **Review and strengthen identity and access controls:** Limit who can access critical systems. Enforce strong authentication and regularly review permissions.
- **Prepare for incidents before they happen:** Test response plans, train and prepare teams, and assume breaches will occur. Focus on fast containment and recovery.

WORKFLOW AND CHATBOT VULNERABILITIES

Businesses introducing AI into their workflow also expose themselves to risk. Unauthorised use of chatbots trained on commercially sensitive or personal information can enable access to bulk data of a sensitive nature. Similarly, chatbots exposed to the public, for instance to lower customer support barriers, may be 'jailbroken' through maliciously crafted prompts to reveal underlying data or logic, unintended for public consumption. This threat is now so pervasive that a leading cyber defence organisation, the MITRE Foundation, has updated its response framework to document and enable defence against malicious activity targeting AI agents.

Long Term Benefits of AI

In the longer-term AI has potential to assist network defenders by strengthening their ability to protect systems at scale and pace.

AI will be most effective when used to augment and strengthen existing tools and processes, not as a standalone solution or a replacement for cyber security fundamentals. Human oversight, governance and policy remain essential particularly where decisions relate to high-value information or high-consequence environments.

Much of the focus on frontier AI has been around its capability to test code for vulnerabilities prior to deployment. While this is an important use-case, the benefits of deploying AI in a deliberate and well-governed way extend across the cyber-defence spectrum. For example:

- Defenders can use AI to baseline resource utilisation, assets and user behaviour to detect anomalous activity in traffic or host systems.
- Enhanced monitoring of data by AI can enable early identification of attacks, enable triage of impact and support faster response and recovery.
- Using AI to reduce repetitive manual processes or improve risk prioritisation can enhance the capability of cyber defence teams in an increasingly complex and fast-moving threat environment.

Most organisations that use AI for business purposes or to enhance cyber security will purchase these tools or services from a third-party supplier. When procuring these tools or services organisations should ensure that suppliers are building in security from the outset, not as an added afterthought. Organisations should also test AI tools to ensure they operate as intended in their environment. Supply chain risks from the adoption of AI need to be actively managed, as do the business risks should AI tools be compromised or services interrupted.

What should leaders do?

Don't wait for more information, or the newest AI tools. Start preparing now.

Cyber threats are a business issue for Chief Executives and governance bodies. The impact of a cyber incident can undermine the confidence of investors, regulators and customers, disrupt operations and have severe financial impacts to a business. In the infrastructure sector the potential risks can extend to community, regional or even national disruption.

Leaders need to be having conversations now, not only with IT and cyber security teams, but across their organisations, to ensure the risks of AI are identified and appropriately treated. The imminent arrival of frontier AI tools makes this focus more urgent.

Questions leaders should be asking:

1. Do we have the people and resources to support an increased tempo of system patching and updates caused by frontier AI?
2. Are we using AI chatbots or other AI tools? How do we manage and protect sensitive data used in these tools?
3. Are we confident our suppliers are building and supplying systems that are secure by design?
4. Do our business continuity plans and crisis response plans factor in cyber attacks and business disruption? Have we exercised these responses?
5. Are our leaders, both in governance and operations, regularly discussing and planning for disruption?

FIVE EYES CALL TO ACTION ON AI

In June 2026 the leaders of the Five Eyes cyber security agencies issued a joint Call To Action about the accelerating cyber security risk caused by frontier AI.

The Five Eyes is a grouping of the national security agencies of Australia, Canada, New Zealand, the United Kingdom and the United States. The agencies rarely issue joint statements but did so on this occasion because of the significant risks to businesses and organisations from the rapidly changing capability of frontier AI models.

The Call To Action stated that cyber resilience is integral to advancing business continuity, market confidence and long-term value. It urged leaders to:

- Understand and assess risk, readiness and accountability
- Prioritise foundational cyber security practices and controls
- Empower cyber leaders with authority and resources
- Stay actively engaged as threats and guidance evolve.

EXAMPLE

In November 2025 Anthropic announced it had disrupted a threat actor, who it assessed was a People's Republic of China (PRC) state-sponsored group, from using AI's agentic capabilities to infiltrate around thirty global organisations. According to Anthropic, the espionage campaign targeted organisations in technology, finance, manufacturing and government sectors including some operators of critical infrastructure. Anthropic assessed the attack had some success.

Anthropic stated that the threat actor manipulated an AI model to bypass safeguards against malicious use and used the model's agentic capabilities to execute parts of the attack without human intervention. Anthropic's assessment was that the use of agentic AI enabled the attack to be undertaken at unprecedented speed and scale.

The key elements of the attack included remote reconnaissance of systems and infrastructure, identifying and testing vulnerabilities and exploiting vulnerabilities with custom code written by the AI. The AI then harvested data and prepared documentation to enable further exploitation of vulnerabilities.

Resources

For further information, refer to the following guidance and advice:

Opportunities for AI in Cyber Defence

This publication provides a guide to how organisations can use AI to strengthen organisational cyber security while managing the risks of using AI.

https://www.ncsc.govt.nz/protect-your-organisation/opportunities-for-ai-in-cyber-defence/

Frontier AI

Managing the increasing risks from vulnerabilities. This guidance is aimed at network defenders and outlines how to manage the increasing risk from vulnerabilities discovered with the introduction of frontier AI.

https://www.ncsc.govt.nz/protect-your-organisation/frontier-ai-managing-the-increasing-risks-from-vulnerabilities/

Cyber Readiness in the Frontier AI era

This advice is designed to help cyber security decision-makers in New Zealand government agencies prepare for the implications of frontier AI products.

https://www.ncsc.govt.nz/protect-your-organisation/cyber-readiness-in-the-frontier-ai-era/

The Implications of Frontier AI Models for Cyber Defence

This advice provides support to senior leaders and network defenders on the implications of frontier AI products.

https://www.ncsc.govt.nz/protect-your-organisation/the-implications-of-frontier-ai-models-for-cyber-defence/

Careful Adoption of Agentic AI Services

This guidance discusses key cyber security challenges and risks associated with the introduction of agentic AI into IT environments, as well as best practices for securing agentic AI systems.

https://www.ncsc.govt.nz/protect-your-organisation/careful-adoption-of-agentic-ai-services/

Artificial Intelligence and Machine Learning: Supply Chain Risks and Mitigations

This guidance is to help organisations when developing or incorporating AI and ML into their systems.

https://www.ncsc.govt.nz/protect-your-organisation/artificial-intelligence-and-machine-learning-supply-chain-risks-and-mitigations

Artificial Intelligence Guide for Small Businesses

This joint guidance has been developed to help small businesses understand the cyber security implications of using AI through applications like OpenAI's ChatGPT, Google Gemini, and Microsoft Copilot.

https://www.ncsc.govt.nz/protect-your-organisation/ai-guide-for-small-businesses/

Principles for the Secure Integration of Artificial Intelligence in Operational Technology

This joint guidance provides critical infrastructure owners and operators with practical information for integrating AI into OT environments.

https://www.ncsc.govt.nz/protect-your-organisation/principles-for-the-secure-integration-of-ai-in-ot/


INTRODUCTION

State-sponsored cyber activity is a persistent threat to New Zealand organisations and businesses

He mōrea tūroa ngā mahi ipurangi taihara a ngā kāwanatanga o tāwāhi ki ngā whakahaere me ngā pakihi o Aotearoa

State actors and their enablers are undertaking malicious cyber activity against New Zealand. The techniques they use are sophisticated and persistent, targeting both government and private sector organisations.

State actors are motivated by national priorities which may include diplomatic or military advantage, economic interests or suppression of dissent. In New Zealand the primary focus of state activity has been espionage, but internationally our partners have identified state actors using cyber tools to undertake intimidation, intellectual property theft, the disruption of networks and critical services, and in some cases, sabotage.

Changing strategic context

State-sponsored cyber activity is happening in the context of a changing threat environment driven by geostrategic competition, conflict and international tensions. In this environment the use of cyber as an offensive tool, or the threat of its employment, can be a mechanism states deploy when faced with a worsening political climate or a deterioration of international relations.

There is a concerning trend by state actors toward more aggressive and assertive activity in cyberspace. This is evidenced by the targeting of critical infrastructure such as energy and telecommunications networks, transport networks, water and financial systems. Actions such as the pre-positioning of offensive cyber capabilities on target systems or limited demonstrations of an attack capability, can be used as a deterrent, and if undetected can limit the warning time to identify and prevent a disruptive attack.

Taken together these actions are challenging the norms of responsible state behaviour in cyberspace. We anticipate that these trends are likely to continue, with AI enabling a significant increase in the volume of these types of operations. This trajectory is likely to create a more volatile and unpredictable environment during periods of conflict.

Why does this matter?

State-sponsored espionage against New Zealand government agencies, businesses and other organisations is a significant risk to our economy, long term security, and ability to shape the world toward our preference for a rules-based international system.

Our location and distance from areas of conflict does not make New Zealand immune to the cascading impacts of cyber attacks. In a highly connected world, a cyber attack elsewhere could create direct or compounding impacts such as disruption of telecommunications and transport networks, interruption to supply chains (physical and digital), and the compromise of sensitive information.

The New Zealand and global context

In the past year the National Cyber Security Centre (NCSC) has identified activity, suspected of originating from foreign state actors, targeting New Zealand government agencies, organisations in the health and education sectors, and information technology managed service providers. The NCSC believes these incidents have exposed sensitive New Zealand information to risk. The NCSC has also joined other nations in identifying state-sponsored activity that targets critical national infrastructure.

Twenty three percent (23%) of the incidents of potential national significance dealt with in the 2025/26 year had suspected state-sponsored links. The NCSC has linked activity to suspected state-sponsored actors from the People's Republic of China, Russian Federation, Islamic Republic of Iran and the Democratic People's Republic of Korea (North Korea). Of these nations the People's Republic of China (PRC) is the most persistent and capable state actor undertaking cyber activity in New Zealand.

In April 2026 New Zealand joined nine other countries to warn against the large-scale use by China-affiliated actors of covert networks of compromised devices such as home routers to hide their malicious activity. Also known as 'botnets', these networks enable malicious activity at scale and have been used by PRC affiliated groups known as Volt Typhoon and Flax Typhoon to target infrastructure networks.

In December 2025 New Zealand joined thirteen other nations and the European Union to warn against attacks on US and global critical infrastructure by pro-Russian hacktivist groups with links to the Russian state. These attacks target water and wastewater, energy and food and agriculture organisations.

In August 2025 New Zealand joined twelve other nations in identifying a campaign of malicious cyber activity being undertaken by a PRC state-sponsored group known as Salt Typhoon. The campaign targeted telecommunications, transport and government networks globally by using publicly known vulnerabilities and exposures in networks and edge devices to undertake espionage including the harvesting of data, phone calls, credentials and network information. Salt Typhoon activity was observed in New Zealand.

THE PACIFIC

Increasing geo-strategic competition is being seen in the South Pacific where we are aware of state-sponsored cyber espionage targeting governments and infrastructure.

New Zealand is a Pacific country with family, cultural, political and economic links to South Pacific nations with whom we share a common interest in fostering regional stability and peace. It is concerning to see Pacific nations being targeted in ways that could impact citizens, businesses and civic institutions.

TOOLS AND TECHNIQUES

State-sponsored actors use a wide range of tools to achieve their objectives, and they constantly refine their techniques so their activity is difficult to detect and defend against. While some state-sponsored activity can be defended against in the same way as other malicious cyber activity, at the extreme end of the spectrum state actors have access to tools and resources beyond the capability of most network defenders to detect and defend, even with third party support.

There are known links between state actors and cybercriminal networks, with an exchange of tools, information and techniques. For example, credentials stolen as part of a criminal exploit may be purchased or transferred to a state actor who then uses them to undertake espionage or other malicious activity. State actors are also known to use criminal groups as proxies to obfuscate their activities and avoid direct state-level retaliation or international sanctions.

EXAMPLE

RUSSIA-LINKED ATTACK ON POLISH ENERGY INFRASTRUCTURE

On December 29, 2025, a cyber actor undertook a coordinated attack on Polish energy infrastructure, targeting renewable energy systems including windfarms, solar farms and combined energy power plant supplying around 500,000 consumers.

The attacker gained access to industrial control systems through vulnerabilities in internet accessible devices. The attack interfered with control systems, corrupted firmware, and damaged remote terminals.

Poland's Computer Emergency Response Team and other experts linked the attack to Russian state actors based on similarities between the December attack and previous activity linked to Russian government organisations. In July 2026 the UK and EU publicly attributed the attack to the Russian state.

Fortunately, the attack did not disrupt the wider Polish energy network, however it is regarded as a significant escalation in cyber attacks with the intent being disruption and sabotage of critical national infrastructure.

Implications for organisations

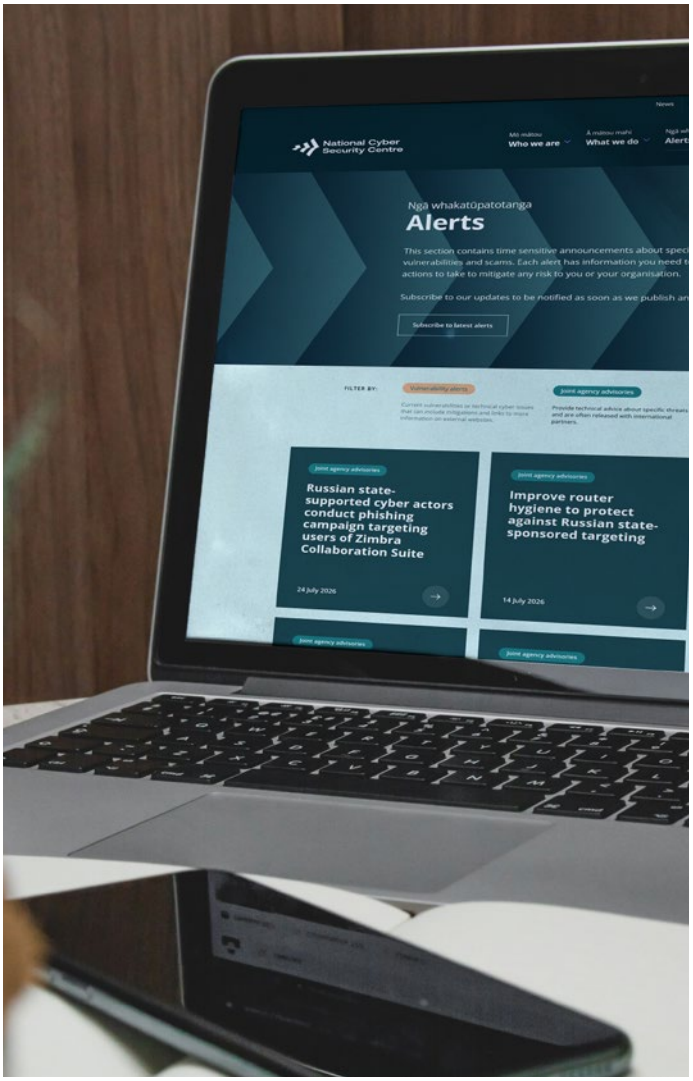
A wide range of New Zealand businesses and organisations are potential targets for state-sponsored cyber espionage or other malicious cyber activity. These include businesses or organisations that operate infrastructure or networks, provide essential services to the public, or hold sensitive information that could provide strategic advantage.

State actors are stealthy and play the long game. Malicious activity can include reconnaissance of systems and the pre-positioning of cyber assets for the purposes of espionage or disruption. The compromise of sensitive information through long-term espionage efforts that are undetected for months or years can have real harm such as compromise of operational technology and the loss of corporate and personal information.

However, even the most sophisticated actors can be foiled by good solid controls. Organisations and businesses, particularly in the infrastructure or network sectors, should regularly review their cyber security settings and be familiar with advice provided by the NCSC on how to identify and tackle counterespionage and state-sponsored activity.

Questions leaders should be asking:

1. Have we considered the risk of intrusion by a sophisticated actor, and the actions we would take to defend against or mitigate such an attack?
2. Are we confident we can detect unusual activity in our environments, including persistent activity over long time frame?
3. Can we identify our mission-critical information assets that need to be protected against state-sponsored threats?
4. Have we reviewed our critical controls recently to understand where we need to put effort to prevent intrusions or compromise of our systems?



Advisories

CHINA-NEXUS COVERT NETWORKS – APRIL 2026

In April 2026 the National Cyber Security Centre joined industry and international partners to advise on how to defend against multiple covert networks which have been created and are being constantly updated by Chinese cyber actors.

PRO-RUSSIA HACKTIVISTS CONDUCT OPPORTUNISTIC ATTACKS AGAINST US AND GLOBAL CRITICAL INFRASTRUCTURE – DECEMBER 2025

In December 2025 the NCSC joined international partners in identifying pro-Russia hacktivist groups conducting cyber operations against numerous organizations and critical infrastructure sectors worldwide. Among the increasing number of groups, some appear to have associations with the Russian state through direct or indirect support.

SALT TYPHOON – AUGUST 2025

In August 2025 the NCSC joined international partners in drawing global attention to a campaign of malicious activity being undertaken by PRC state-sponsored cyber threat actors targeting networks globally, including, but not limited to, telecommunications, government, transportation, lodging, and military infrastructure networks.

Resources

For further information, refer to the following guidance and advice:

New Zealand Information Security Manual

The NZISM explains processes and defines controls essential for protecting New Zealand government information and systems. Crown entities, local government and private sector organisations are also encouraged to use the NZISM.

https://nzism.gcsb.govt.nz/

Government Information Security Framework and Policies

The Information Security Framework is a part of the New Zealand Government's Protective Security Requirements (PSR), a best practice security policy framework for security governance

https://www.protectivesecurity.govt.nz/policy/information-security

CASE STUDY 1

NORTH KOREAN IT WORKERS IN NEW ZEALAND

During the year a large New Zealand business became suspicious of the identity details of an IT contractor working remotely.

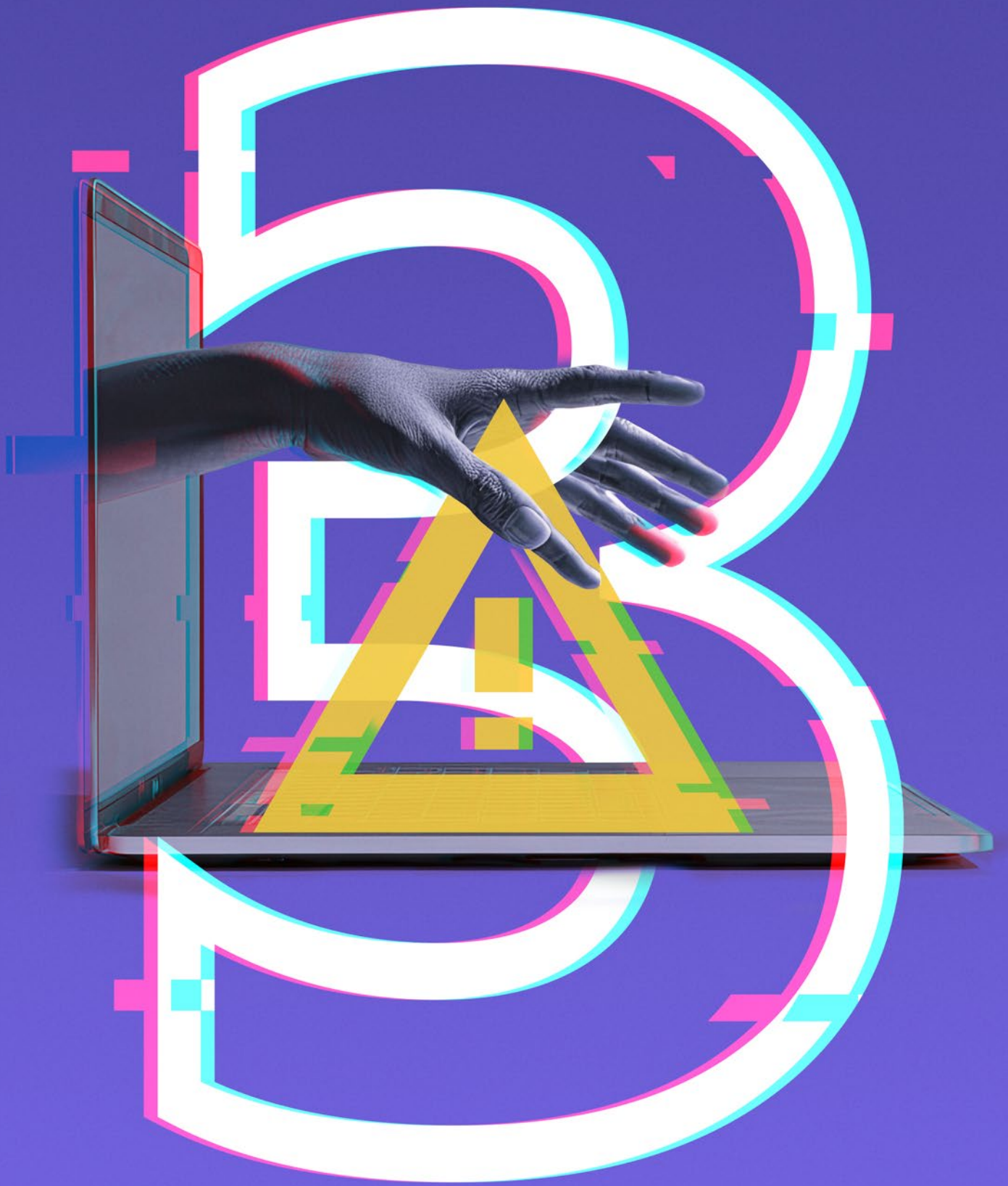
The business contacted the NCSC and New Zealand Police, and investigation identified the worker as being from North Korea (Democratic People's Republic of Korea or DPRK). To gain employment the North Korean worker used a false persona including fake identity documents, a New Zealand address as a contact point and recruited a New Zealand citizen to receive and operate the company's laptop.

The New Zealand business immediately terminated the employment of the North Korean worker and refused to pay for their services. The worker then claimed to have obtained commercially sensitive information and threatened to release this if not paid.

The North Korean state operates a coordinated programme of using remote IT workers to generate revenue for the regime, including the funding of sanctioned weapons programmes. In some cases, the workers also undertake malicious cyber operations. These workers often operate under front companies overseen by the North Korean state apparatus. The IT workers use identity masking technology to hide their North Korean identity when securing contracts for remote work.

North Korea is currently subject to UN sanctions which have effect in New Zealand law. These sanctions impose various restrictions and prohibitions including a prohibition on granting work visas to North Korean nationals, and a prohibition on the export of data and software to, for use in, or for the benefit of North Korea.

To mitigate the risk of employing North Korean IT workers organisations should consider interviewing potential staff face-to-face and require new staff to pick up IT equipment personally. Other risk factors to be aware of include requests to be paid in cryptocurrency, refusal to participate in video-conference meetings and the recording of unusual working hours.



Cybercrime and extortion are escalating in severity

Kei te kino haere kē atu te taihara ipurangi me te mure

In the twelve months to June 2026, New Zealand experienced more high-impact cybercriminal activity than in the past five years. This activity included high-profile attacks on health service providers and tertiary institutions.

Of the 369 cyber incidents of potential national significance reported to the National Cyber Security Centre (NCSC), 162 had links to criminal or financially motivated actors, a jump of 18% over the previous year. Of these cyber incidents, four were classified C2, or highly significant, the first cybercrime incidents of this severity for five years. High profile incidents include the theft of over 99,000 patient records from the Manage My Health patient portal, and the breach of the Canvas learning management system used by some of New Zealand's largest educational institutions.

While some cyber attacks are complex, most common cybercrime could be prevented if businesses and organisations took simple actions to protect credentials and identify data, using tools such as multi-factor authentication, long strong passwords, passkeys and software allow lists.

Why does this matter?

Cybercrime has a significant impact on individuals, businesses and organisations. The impact includes direct financial costs to businesses, the theft of private and sensitive information, financial scams and espionage.

For individuals the theft of sensitive personal information, such as health records, legal or financial information or identity data, can be distressing. Once stolen this information is often resold by cybercriminals, creating a long tail of risk for individuals.

For businesses and organisations, a cyber attack can have significant impacts including disruption of operations, a loss of trust among customers and clients, investigations by regulators and financial impacts from loss of business. Containing and remediating cyber attacks can be costly in both financial terms and in the impact on staff.

CYBERCRIME HAS MAJOR IMPACTS ON NEW ZEALANDERS

- In December 2025 the NCSC contacted 26,000 New Zealanders to warn them their credentials had been stolen by a malware known as Lumma Stealer, a credential stealing tool linked by open-source assessments to criminals operating in Russia.
- In February 2026 the operation of many aged care facilities, hospices and community pharmacies was disrupted when the medication management platform MediMap was hacked. The attackers altered some patient records, and normal medication distribution was disrupted while the system was offline.
- In May 2026 the Canvas learning management system, used by some of New Zealand's major tertiary education providers, was breached in a supply chain attack. It is estimated that data and identity information was stolen from between 110,000 and 120,000 students and staff.

Why is cybercrime on the increase?

The cybercrime landscape is dynamic and responds quickly to changes in technology, enforcement and economic incentives.

Cybercrime is now an industrialised, global industry in which advanced malware and tools are available for purchase or rent as a service and are sometimes customised to exploit the vulnerabilities of particular targets. Some cybercriminals are using sophisticated tools to plan and orchestrate attacks thereby reducing the effort expended on individual exploits.

Cybercriminals are becoming more capable and considered in their efforts to evade detection. Some of the capabilities and techniques being utilised make it challenging for the victim to identify what has been stolen and by whom.

Cybercriminals have become more aggressive in their pursuit of monetary payment, via ransoms or extortion. The tactics include:

- Targeting individuals
- Increased harassment of potential victims
- Increased focus on theft and exposure of highly sensitive information (such as health, legal or insurance records)
- Greater focus on victims with a low tolerance for disruption, such as infrastructure or health service providers.

CASE STUDY 2

Malware-as-a-Service
Lumma Stealer

In December 2025 the NCSC alerted over 26,000 New Zealanders that their devices had been infected with malware known as Lumma Stealer which is designed to steal sensitive information like passwords and login details for online accounts.

Lumma Stealer is an example of 'Malware-as-a-Service' or MaaS. Cybercriminals purchase the software, paying as little as $250 for a subscription, or up to $20,000 for customisation and concealment options. The user then targets online communities, education systems and organisations, and businesses across multiple sectors, including critical infrastructure.

It's likely the affected people unknowingly downloaded the malicious software by clicking a link within a phishing email or downloading the software from a compromised website. Some of the stolen passwords were connected to government agency systems and bank accounts.

Open-source assessments link Lumma Stealer to Russian crime networks and identify its use by state-affiliated criminal groups in Russia and China to undertake espionage against infrastructure-related organisations including gathering identity credentials, crypto-currency wallets and two-factor authentication (2FA) browser extensions.

Monitoring threats

In a constantly developing threat landscape, businesses may wish to consider the use of tools or services that monitor areas where breached data may exist. These places may include the dark web, known hacking or online forums, and communication or channels such as Telegram and WhatsApp. For most businesses having an external cyber-security supplier will be the most cost- effective way to provide visibility of threats and inform their approach to cyber defence.

Cybercriminals operate internationally, sometimes in coordination with states

Cybercrime is an international enterprise. Attacks targeting New Zealanders can originate from almost anywhere on the globe, and stolen data will be sold internationally for use in future attacks, by criminal or state-affiliated actors.

While most cybercriminal activity is financially motivated there is evidence that state actors enable and support cybercriminals, and use data stolen by criminals for other state purposes. For example, the individuals or group behind Lumma Stealer are Russian in origin, and their tools have been used by criminal groups affiliated with both Russia and the People's Republic of China.

DATA AND CREDENTIAL THEFT – A GROWING FOCUS FOR CYBERCRIMINALS

Theft of data and credentials is becoming more common as cybercriminals seek to extort ransoms from organisations and individuals. The more personal or sensitive the information the more likely an organisation or individual will pay a ransom. This explains the focus of cybercriminals on organisations in the health services sector holding highly personal information.

Because stolen data may contain sensitive personal or business information it can be monetised in several ways including immediate attempts to extort a ransom or sale to another actor for use in targeting or accessing victims.

Credentials are less valuable individually but are sold on global markets in large numbers where they can be purchased and reused by other cybercriminals or state actors leading to cascading harm to individuals or organisations.

The payment of ransoms does not guarantee the recovery of data or the destruction of stolen information. An international survey of 5,750 businesses by UK insurer Hiscox Ltd indicates that approximately 40% of victims who paid a ransom fail to recover data and approximately 80% of organisations that paid ransoms were attacked again, often by the same attacker or a related group.

Artificial Intelligence is part of the cybercrime toolkit

Attackers are beginning to leverage Artificial Intelligence (AI) in combination with social engineering to create threats that are increasingly difficult to detect and remove.

State actors and cybercriminals are already using AI to develop more authentic phishing messages and scams, undertake more effective reconnaissance of targets, and increase the volume and scale of attacks.

In 2025, we have seen the emergence of AI-powered malware: code that can make simple decisions without human oversight. This new breed of programmes can adapt automatically to new security environments, avoid detection by rewriting sections of their own code, and choose their own target when an opportunity presents itself.

HOW DO CYBERCRIMINALS TARGET NEW ZEALANDERS?

Cybercrime affects New Zealand in multiple ways. These are some of the most common:

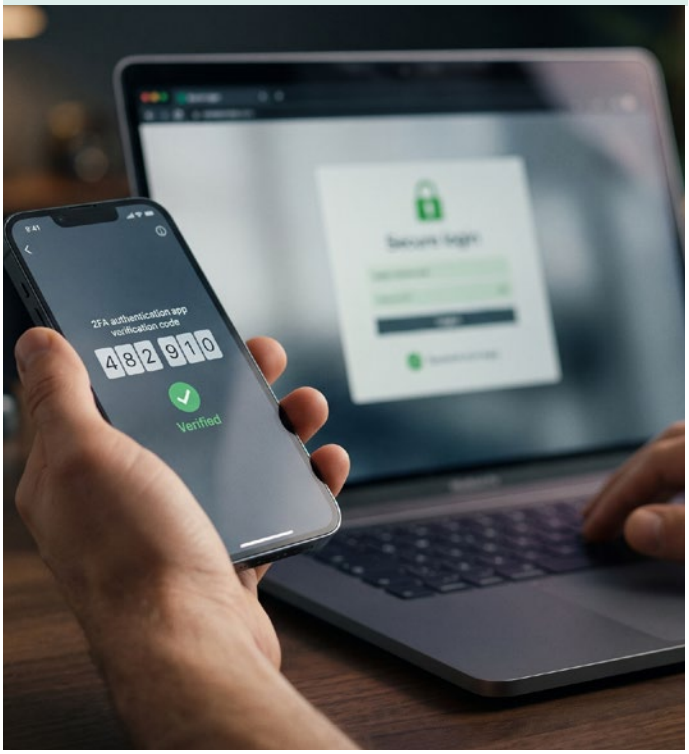
- **Extortion.** Cybercriminals extort money from individuals or businesses, usually by demanding money to avoid the leaking of sensitive information. Other methods include encrypting user data or systems and demanding money to restore the system.
- **Credential theft.** Credentials are stolen from a user or business, and then the criminal monetises through extortion, and often the resale of the credentials. The reuse of stolen credentials is common and can lead to further attacks.
- **Scams:** Cybercriminals trick the victim into sending money, sharing sensitive information, or purchasing a bogus product or service. These scams often rely on the use of stolen credentials or social engineering techniques such as seemingly authentic messages to deceive the victim.

Implications for organisations

The impact of cyber attacks on businesses and organisations can be severe including long-term damage to customer trust and business reputation, disruption of services and direct costs to remediate and restore systems.

Three questions leaders should be asking

1. Have we ensured that access credentials are secure and well managed?
2. Is our software patching up to date, and known vulnerabilities addressed?
3. Do we have the management and business continuity systems in place to manage a cyber attack?



CASE STUDY 3

MANAGE MY HEALTH

In late December 2025 a cybercriminal gained access to the Manage My Health (MMH) Patient Portal Web App, using a valid user's credentials (username and password). These credentials had been stolen through a malware infection known as Lumma Stealer.

As a result of the attack sensitive health and personal information of more than 99,000 New Zealand patients was stolen. The Ministry of Health assessed that the scale and sensitivity of the data involved made this one of the most serious cyber security incidents experienced in New Zealand.

Summarising the cyber security reviews it commissioned, the Ministry of Health concluded that the breach itself was largely preventable, and the review observed that this type of attack was neither technically sophisticated, nor particularly uncommon.

The review identified weaknesses in crisis communications, incident preparedness and technical controls. In particular, multi-factor authentication while available was not mandatory for all users and other user access controls were not implemented.

Cyber security basics are essential

The NCSC's assessment is that this example highlights the importance of implementing basic cyber security processes and systems as the first line of defence against cybercriminals and other malicious actors. Credentials compromised in a separate incident were the initial entry point for the Manage My Health attack, which then enabled the criminal actor to exploit flaws in a component of the portal to obtain patient information.

Since the attack, Manage My Health has acknowledged the serious nature of the incident and has implemented security and operational improvements including mandatory multi-factor authentication for all users, enhanced real-time monitoring, strengthened access controls, and expanded independent security testing across the platform. This incident demonstrates how compromised credentials, when combined with weaknesses in security controls, can result in significant impacts. It also reinforces the importance of organisations continuously assessing whether security controls remain effective to defend against a rapidly changing threat landscape.

Resources

For further information, refer to the following guidance and advice:

Cyber Security Guidance for High-Profile Individuals

If you have a high-profile job or are well-known, you may be more likely to be targeted by cybercrime. This guidance will help you know what to watch out for, and how to protect yourself online.

- https://www.ncsc.govt.nz/protect-your-organisation/cyber-security-guidance-for-high-profile-individuals/

Protect your Organisation against Ransomware

Ransomware attacks are becoming increasingly common and sophisticated. This guidance explains how you can stop a ransomware attack in its tracks.

- https://www.ncsc.govt.nz/protect-your-organisation/protect-your-organisation-against-ransomware/

Response Planning

Organisations have in place a process to develop and test cyber incident management plans to ensure business continuity in the event of system or service failure.

- https://www.ncsc.govt.nz/protect-your-organisation/response-planning/

You can't defend what you don't know: Digital supply chains continue to be a major risk to New Zealand businesses

Tē taea e koe te kaupare i ngā mea kāore koe i te mōhio: He tūraru nui ngā ara tukutuku matihiko ki ngā pakihi o Aotearoa

Digital supply chain compromises have been responsible for major incidents in New Zealand in the last year affecting business operations and potentially resulting in loss of personal information and identify data for hundreds of thousands of users.

Digital supply chain breaches happen when software, hardware or other services provided by third-party vendors are compromised by cybercriminals or other malicious actors. The compromise then allows an attacker to access data or systems used by a target organisation. Targeting supply chain vendors is a strategy used by both financially motivated criminals and state-sponsored actors to access multiple targets.

Why does this matter?

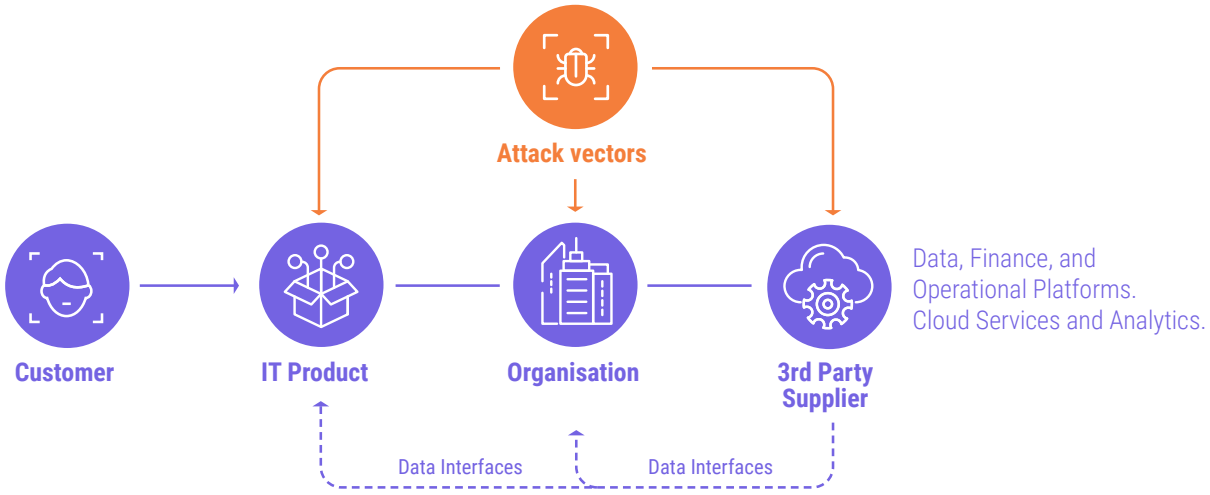
Many organisations are now reliant on a mix of platforms, suppliers, outsourced services and digitally controlled technologies to run their operations. Many of these suppliers will be based overseas and it's unlikely that many New Zealand organisations have visibility of their cyber security settings such as access controls, patching cycles or data encryption.

A single security failure at the vendor level, here or overseas, can cascade to potentially multiple compromises of data and operational systems in New Zealand. These compromises might be unexpected and significant.

Supply chains are an attractive target

Attacks via third-party suppliers are an attractive vector for cybercriminals. One reason is that successfully infiltrating the defences of a service provider may allow the attacker to circumvent the defences of a client, who is their main target. Secondly, compromising the systems of a supplier may provide access to many client organisations, greatly expanding the scale of a breach.

Supply chain risks also apply to Operational Technologies (OT) controlling industrial processes and physical operations. These systems are increasingly connected directly to the internet and can also be connected to internal networks creating a new vector for compromise. The software and control systems for OT can be vulnerable if not protected and managed at the same level as corporate systems. In the past year sabotage and disruption of OT systems in the energy sectors of several countries has been attributed to Russian state actors.



Complex supply chains also create broader attack surfaces for malicious cyber actors, with third party applications managing data, finances and other valuable information offering potential targets. When these applications have data interfaces within an organisation, this creates pathways that could be exploited to infiltrate ransomware or malware into networks.

Another attack vector observed in large data breaches is customer service or IT support services provided by third parties. These services have access to networks and data and have been targeted by malicious actors to gain access to internal systems. The Qantas data breach in 2025 was the result of a sophisticated attack on an IT support service, combined with the infiltration of malware into a third-party system.

What's the current landscape?

In the past year several New Zealand organisations have been victims of attacks by cybercriminals exploiting third party suppliers or systems. The healthcare sector has been targeted on multiple occasions with a focus on accessing and stealing sensitive personal information held on third party applications for the purpose of extortion. It is also likely that data stolen in these exploits is retained by the criminals involved, or sold to other actors, for the purposes of mining credentials and other information, or for secondary extortion of victims.

A developing risk lies with the unsanctioned or unintended exposure of data through the use of Artificial Intelligence (AI) tools. Data leakage can result from the storage of information in locations lacking appropriate security controls, limiting defender oversight and ability to respond.

The compromise of third-party vendors or software providers as part of a broader campaign of espionage or disruption by state-sponsored actors is a realistic possibility as the global environment becomes more contested. New Zealand organisations may not be the primary target of such activity, but compromise in the digital supply chain may affect availability of networks or services or could compromise information irrespective of whether there was a deliberate intention to impact us.

Across many cyber incidents the common factors are lack of authentication (e.g. not using multifactor authentication), over-permissioned access to systems (i.e. more people have access than necessary), and poor separation or segmentation of data. Implementing the following basic security controls provides a strong basis for protection from common attacks:

- Enabling appropriate firewall protection
- Encrypting data
- Enforcing multifactor authentication on all systems, accounts and profiles
- Setting access limitations on accounts, or adhering to the principle of least privilege (limiting who is authorised to access what)
- Enabling data loss prevention solutions for data at rest (to help prevent personal information from getting out)
- Patch management
- Network segmentation.

CASE STUDY 4

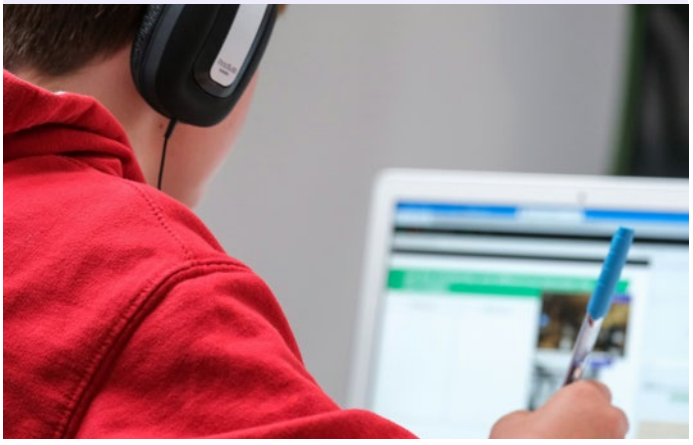
CANVAS LEARNING MANAGEMENT SYSTEM

In May 2026 a US-owned cloud-hosted learning management system called Canvas suffered a security breach in which cybercriminals accessed user information and then posted messages on users' login pages demanding ransom payments.

The breach immediately affected millions of users globally, including over thirty New Zealand tertiary institutions, schools and other education system suppliers. The Ministry of Education estimates that between 110,000 and 120,000 students and staff were affected by the breach, which resulted in the temporary loss of services, and the theft of names, emails, student IDs and messages exchanged between users.

The New Zealand institutions who used Canvas as their learning management system lost the ability for students and staff to undertake essential tasks such as delivering course information, submitting assessments, reviewing and grading assessments, and communicating between individuals and groups.

This incident highlighted the vulnerability of institutions to disruption of essential services provided by offshore partners, and the limited options available to them to mitigate the impact. It took several days for the US-based operator to restore services, during which time communications and information were very limited.



Implications for organisations

Supply chain threats are difficult to avoid and therefore basic cyber security requirements remain essential, as well as specific control measures such as Software Bill of Materials and assessing cyber security as a component of awarding supplier contracts.

For organisations where third-party suppliers or applications hold sensitive data, operate essential equipment or are business critical, a strong understanding of the cyber security risks in the supply chain is essential. Developing this understanding can be done when services are contracted and form part of the discovery and assessment process during procurement.

Questions leaders should be asking:

1. When you contract third-party suppliers do you assess their cyber security as part of the procurement process?
2. Have you exercised or planned a response to a data breach or operational compromise of a third-party application?
3. Do we have ongoing assurance that suppliers are maintaining agreed levels of cyber security?
4. Do you have specific contractual clauses with your supplier that establish clear data protection and cyber security expectations?

Resources

For further information, refer to the following guidance and advice:

Responding to Third-Party Data Breaches

If you suspect your organisation is affected by a third-party data breach, the NCSC has advice on the steps to help manage the risk.

https://www.ncsc.govt.nz/protect-your-organisation/responding-to-third-party-data-breaches/

Supply Chain Cyber Security: In Safe Hands

This advice describes the basic controls which need to be in place, and detailed questions to ask suppliers, to implement and maintain fundamental cyber security controls in Supply Chain management.

https://www.ncsc.govt.nz/protect-your-organisation/supply-chain-cyber-security-in-safe-hands/

Keeping Personal Information Safe: A Guide for Organisations and their Suppliers

The following advice is designed to help organisations implement appropriate controls when working with third-party suppliers.

https://www.ncsc.govt.nz/protect-your-organisation/keeping-personal-information-safe-a-guide-for-organisations-and-their-suppliers/

Artificial Intelligence and Machine Learning: Supply Chain Risks and Mitigations

Joint guidance reflecting that adopting Artificial Intelligence (AI) and machine learning (ML) systems introduces unique supply chain risks, which can threaten the cyber security of an organisation, if not securely managed.

https://www.ncsc.govt.nz/protect-your-organisation/artificial-intelligence-and-machine-learning-supply-chain-risks-and-mitigations/

Software Bill of Materials (SBOM) for Cyber security

This joint guidance describes why organisations should consider adopting a Software Bill of Materials (SBOM).

https://www.ncsc.govt.nz/protect-your-organisation/software-bill-of-materials-sbom-for-cybersecurity/


VICTOR
11:24 AM
Date: Oct 26

Social engineering is a persistent threat to organisations and businesses

Ko te rāwekeweke pāpori tētahi tuma tūroa ki ngā whakahaere me ngā tāngata

Social engineering is a persistent and effective technique used by malicious actors to gain access to networks, to steal information and to defraud individuals.

Artificial Intelligence (AI) is making it easier to create and deploy sophisticated social engineering attacks. These attacks include highly convincing deepfakes and the integration of publicly available or stolen data to create more authentic messages to manipulate and persuade targets.

Why does this matter?

Social engineering attacks are sometimes associated with scams and fraud against individuals, but the targets often include multi-national businesses, government agencies and third-party suppliers. In the past year, social engineering techniques have been used to compromise New Zealand healthcare organisations and breach the security of New Zealand government organisations.

Because social engineering targets individuals it is a tool that can successfully bypass physical or software defences. The targeting of IT support services and help desks has proven a highly effective vector for cybercriminals seeking a high-leverage low-resistance entry point to corporate networks.

What's the current landscape?

Social engineering attacks can be meticulously planned and use sophisticated multi-step techniques to obtain credentials and infiltrate networks. The use of AI tools to undertake reconnaissance of individuals or organisations and personalise messages by combining harvested or stolen data with AI impersonation, is another way in which social engineering techniques are becoming more convincing and effective.

Techniques and tactics are evolving with the use of generative AI providing cybercriminals and other malicious actors with new tools to persuade, manipulate and deceive individuals. These include:

- Generating extremely convincing phishing messages or fake websites
- Generating scam phone calls in which you talk with an AI directly
- Mimicking writing styles, corporate branding, and slang used by particular communities
- Translating scam messages or voice calls into other languages.

Social engineering techniques include the impersonation of a trusted person or organisation, the use of emotional language or messages, and pressuring victims to take actions in a short time frame. Social engineering can be done by email, on collaboration platforms such as Microsoft Teams or by using audio or video tools including deepfakes.

If AI tools ultimately enable stronger cyber defences at the software layer, then social engineering will become a more important vector for criminals and other malicious actors to obtain credentials and breach cyber security.

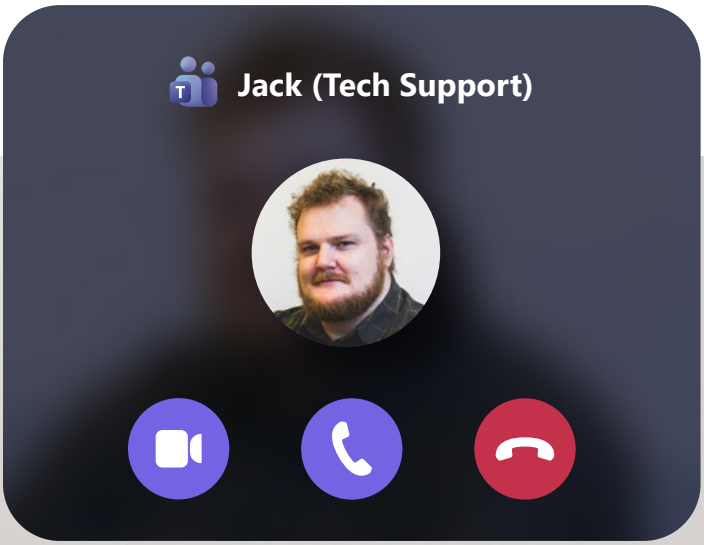
CASE STUDY 5

TARGETING IT PROFESSIONALS

Technically literate individuals can fall victim to social engineering techniques, and some social engineering lures are tailored to these victims.

During the past year the NCSC received a small number of reports about information technology (IT) professionals being approached under the pretext of a job opportunity. While victims think they're doing a skills test for a new IT or programming role, the source code they download can contain malware.

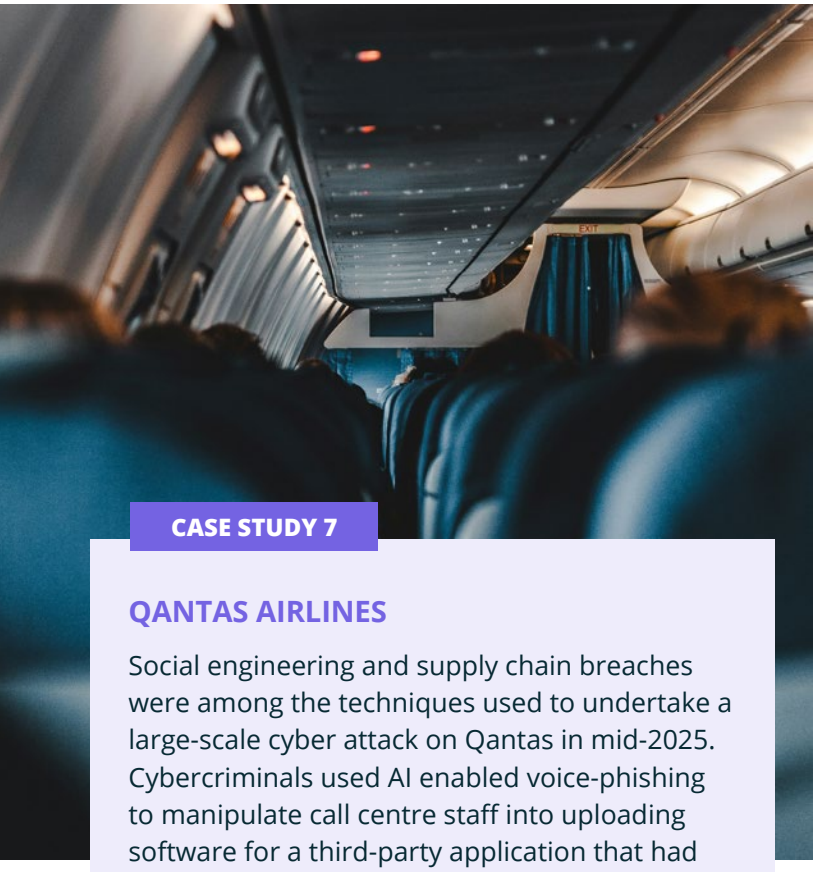
Those who reported this activity to the National Cyber Security Centre (NCSC) had identified inauthentic behaviour, although in one case, not before downloading and allowing the malicious code to run. Often this code is hosted in public version control repositories, like Github or Bitbucket, which may provide undue confidence to the victim.



CASE STUDY 6

ONLINE COLLABORATION PLATFORMS

Online collaboration platforms have become another vector for social engineering compromise if they are not effectively locked down. In a case reported to the NCSC a contractor to New Zealand government organisations received an inauthentic 'helpdesk' call via Microsoft Teams. From there, actors socially engineered their access to the contractor's network and installed software that enabled them to evade malware detection and exfiltrate data.



CASE STUDY 7

QANTAS AIRLINES

Social engineering and supply chain breaches were among the techniques used to undertake a large-scale cyber attack on Qantas in mid-2025. Cybercriminals used AI enabled voice-phishing to manipulate call centre staff into uploading software for a third-party application that had been modified to enable data exfiltration.

As a result of the breach information of around 5.7 million customers was stolen by cybercriminals including customer names, addresses, phone numbers, email addresses and frequent flyer information.

Once access had been gained, the integration of the third-party system enabled access to sensitive information. More rigorous access control and data segmentation may have reduced the extent of the breach.

This breach demonstrated that even well-resourced organisations using software provided by major vendors are vulnerable to sophisticated social engineering attacks. In this case the combination of social engineering and supply chain attacks was successful.

Social engineering and supply chain attacks are a persistent vulnerability. Vendors are part of your attack surface.

Implications for organisations

Organisations need to support and train their staff to recognise and be resistant to social engineering attacks. This is true for staff across organisations as well as those working in common attack targets such as call centres and IT service desks.

Social engineering attacks against call centres and IT service desks have demonstrated the effectiveness of these tactics in enabling cyber extortion incidents. Cybercriminals target service desks as a high-leverage, low-resistance entry point into corporate networks.

In addition to supporting staff, organisations can mitigate the impact of breaches by ensuring stronger access controls to limit lateral movement in networks and unnecessary access to data.

Questions leaders should be asking:

1. Has your organisation's access governance been reviewed recently? Do you operate a zero-trust architecture or multi-factor authentication?
2. Are you training your staff to recognise, report and defend against social engineering attacks?
3. Are you confident your organisation's training is regularly refreshed with up-to-date case studies and real-world examples of phishing, vishing or other techniques?

Resources

For further information, refer to the following guidance and advice:

Build Security Awareness in your Organisation

Investing in your people's security awareness and training, alongside implementing technical controls, is a long-term commitment to improving the security of your organisation.

https://www.ncsc.govt.nz/protect-your-organisation/build-security-awareness-in-your-organisation/

Principle of Least Privilege

Many security problems such as credential harvesting and unauthorised access happen when people have more administrative permissions than they need.

https://www.ncsc.govt.nz/protect-your-organisation/principle-of-least-privilege/

Network Segmentation and Separation

Your organisation's network can be physically and virtually configured to add more granular levels of security controls.

https://www.ncsc.govt.nz/protect-your-organisation/network-separation-and-segmentation/

By the numbers

Total incidents reports recorded for 2025/26

4673

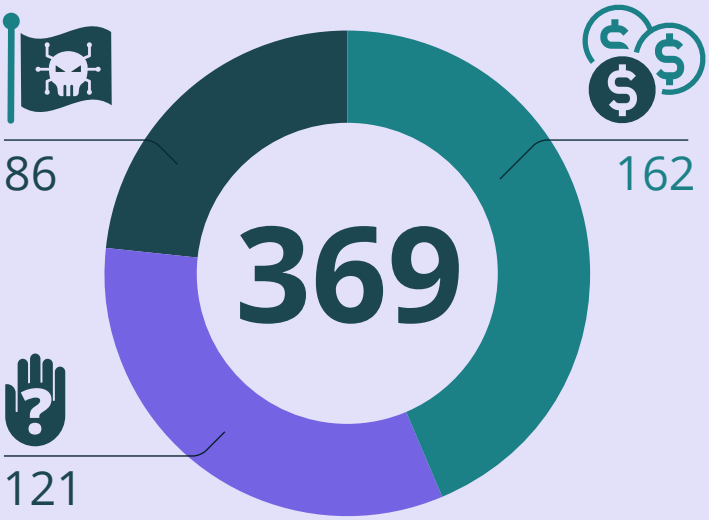
(compared to 5995 in 2024/25)

INCIDENT SEVERITY

- **Highly Significant** 0.1%
- **Significant** 0.7%
- **Moderate** 2.7%
- **Routine** 4.2%
- **Minor** 92.3%

Total incidents triaged for specialist technical support because of potential national significance

(compared to 331 in 2024/25)



Linked to suspected state-sponsored actors

23% ↓ compared to 25% (82) in 2024/25

Likely criminal or financially motivated

44% ↑ Compared to 41% (137) in 2024/25

Incidents could not be linked

33% ↓ Compared to 34% (112) in 2024/25

Direct financial loss recorded

$23.8m

↓ Decrease from 2024/25 of $3.1m ($26.9 million)

Incident Reporting analysis 2025/26
Tātaritanga pūrongo maiki mō te tau 2025/26

New Zealanders can report cyber security incidents to the National Cyber Security Centre (NCSC) through an online portal, which enables us to provide advice about the recommended next steps to those affected. The NCSC receives incidents of all sizes, from phishing up to major cyber security breaches.

INCIDENT TRIAGE

The NCSC handles cyber incident reports through two distinct triage processes. Most incident reports are managed through the NCSC's general triage process.

A small number of cyber incidents are triaged for specialist technical support due to the nature of the victim or the seriousness of the incident. These incidents could cause high impact at the national level and are referred to as incidents of potential national significance. These may be incidents affecting organisations such as operators of critical infrastructure, and incidents that have the potential to impact large groups of New Zealanders.

The following section presents an analysis of cyber incidents reported to us during the period from 1 July 2025 to 30 June 2026. Due to the way incidents are dealt with, some analysis is only available for certain subsets of the data.

WHY REPORT?

Any person or organisation in New Zealand can report incidents to the NCSC, to obtain help and guidance. We can help you understand what has happened, stop the incident getting worse, and help you get back on your feet. Reporting also provides us with information about the threat landscape, which we can use to issue advisories and alerts, or take disruptive action.

Severity and sector breakdowns

In 2025/26, the NCSC received a total of 4,673 reports. Individuals made 3,627 (78%) reports and organisations were responsible for 671 (14%) reports. The remaining did not specify the reporter.

While the total number of cyber incidents reported to the NCSC has declined since 2021 the number of incidents of potential national significance has remained at a similar level. Furthermore 2025/26 saw four incidents classified as C2, or highly significant. The overall decline in reporting of lower severity incidents may reflect a number of factors including the integration of CERT NZ (Computer Emergency Response Team) into the NCSC, changes to how the reporting of phishing incidents is managed and increased reporting of incidents directly to businesses (e.g. customers reporting directly to banks rather than to NCSC) or to other relevant agencies such as the Department of Internal Affairs and New Zealand Police.

INCIDENT SEVERITY

The NCSC triages incidents into six categories ranging from C1 (national cyber emergency) to C6 (minor incident).

In the 2025/26 year, the most severe incidents were categorised as C2. These incidents included the use of compromised credentials to exfiltrate personal information from organisations in the health services sector. These attacks were undertaken by financially motivated cybercriminals.

A national cyber emergency (C1) is defined as an incident that causes severe disruption to a core New Zealand service, and/or affects key sensitive data, and/or undermines the economic or democratic stability of New Zealand. At the other end of the scale, a minor incident (C6) is defined as an incident causing a known or likely impact on an individual / individual, or precursor activity against an individual / individual or a small or medium enterprise. In the middle, a significant incident (C3) is defined as an incident causing a known or likely impact on a large commercial enterprise, wider government, or supply chain to core New Zealand services.

Highly significant incidents (C2) consume substantial time and resources, but even significant (C3) or moderate incidents (C4) can take weeks to resolve and will generally involve complex responses involving several teams. For minor or routine incidents (C5 or C6), the NCSC might respond by providing general advice or alerts to customers.

C6	C5	C4	C3	C2	C1
3872	178	112	30	4	0
Minor incident	Routine incident	Moderate incident	Significant incident	Highly Significant incident	National Cyber Emergency

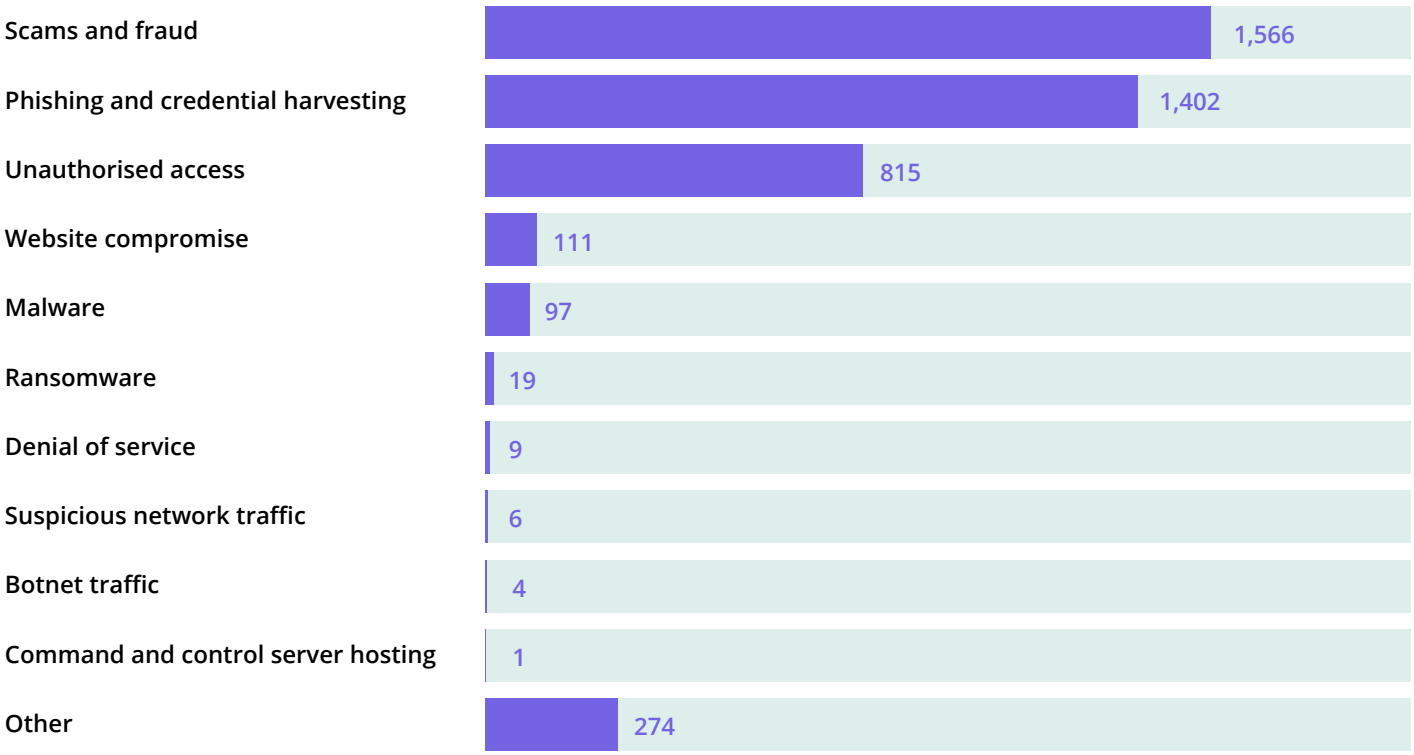
SECTOR BREAKDOWN

The following table shows the sector breakdown of the 4304 incidents handled through our general triage process.

Agriculture, Forestry and Fishing	23
Arts, Recreation and Other Services	42
Construction	39
Education and Training	56
Electricity, Gas, Water and Waste Services	28
Financial and Insurance Services	54
Health Care and Social Assistance	53
Individual	3627
Information Media and Telecommunications	32
Manufacturing	48
Mining	1
Professional, Scientific, Technical, Administrative and Support Services	81
Public Administration and Safety	102
Rental, Hiring and Real Estate Services	11
Retail Trade and Accommodation	51
Technology	18
Transport, Postal and Warehousing	22
Wholesale Trade	10

SUB-CATEGORY BREAKDOWN

The following table shows a breakdown by the type of attack of the 4304 incidents reported to NCSC.



FINANCIAL AND OTHER LOSSES

The NCSC records the direct financial loss reported by victims, whether lost to scams or the cost of recovery, where this information is volunteered.

The direct financial loss reported in 2025/26 totalled $23.8 million, a decrease from $26.9 million in 2024/25. The NCSC has recorded several types of loss amongst the incidents handled through the general triage process:

Financial loss

1278

Includes not only money lost as a direct result of an incident, but also the cost of recovery – for example, the cost of contracting IT security services.

Data loss

220

Loss or unauthorised copying of data, business records, and intellectual property.

Reputational loss

66

Damage to the reputation of an individual or organisation as a result of the incident.

Operational impact

32

The time, staffing and resources spent on recovering from an incident, taking people away from normal business operations.

Technical damage

19

Impacts on services like email, phone systems or websites, resulting in disruption to a business or organisation.

Other loss

67

Includes types of loss not covered in other categories.

Due to the way incidents are handled, not all financial loss information is reported or recorded.

Analysis of incidents of potential national significance

In 2025/26, 369 incidents reported to the NCSC were triaged for specialist support and analysis and are referred to as incidents of potential national significance.

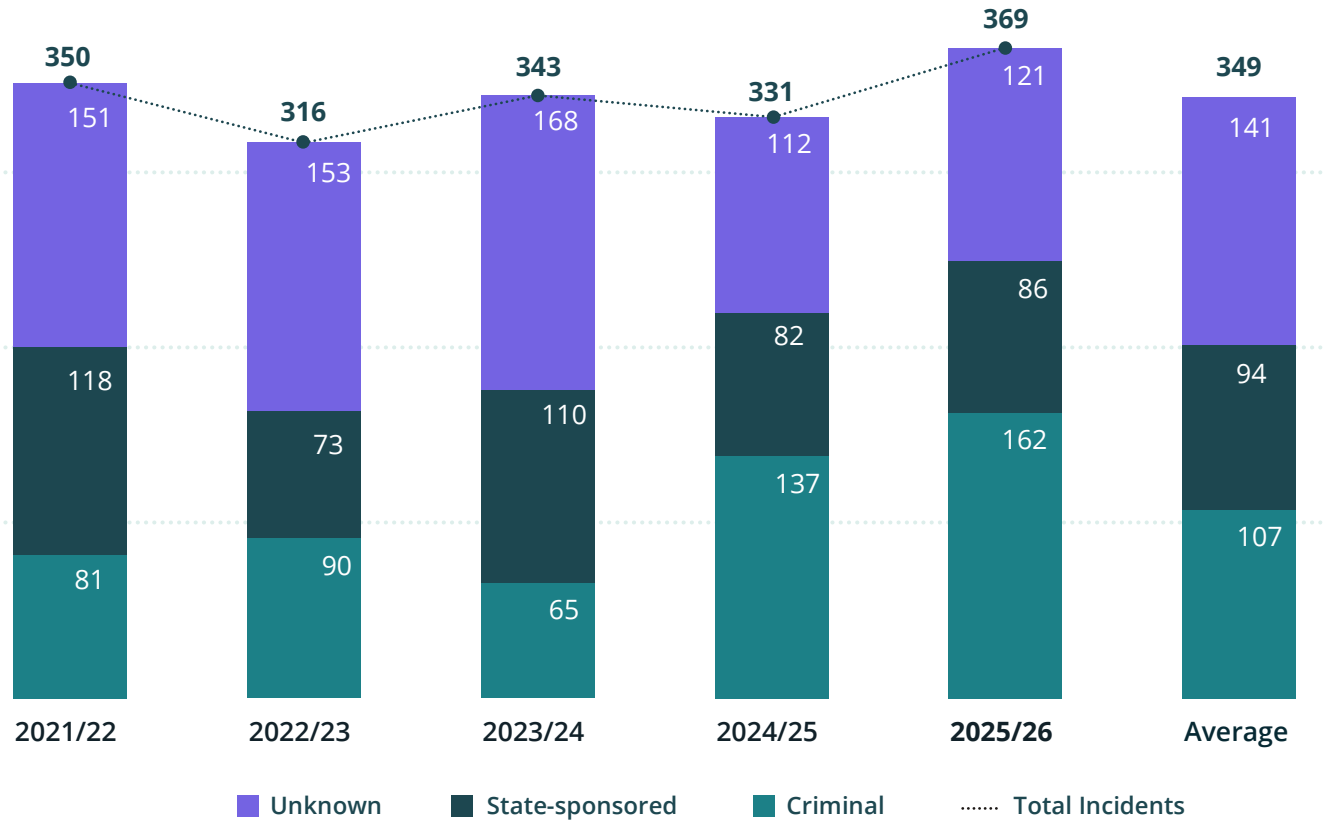
Actor motivations

After several years of decline 2025/26 saw an increase in the total number of incidents of potential national significance handled by the NCSC. An 18% jump in criminal or financially motivated incidents has driven the overall increase.

Out of the 369 reported incidents, 86 indicated links to suspected state-sponsored actors, compared to 82 in the 2024/25 year.

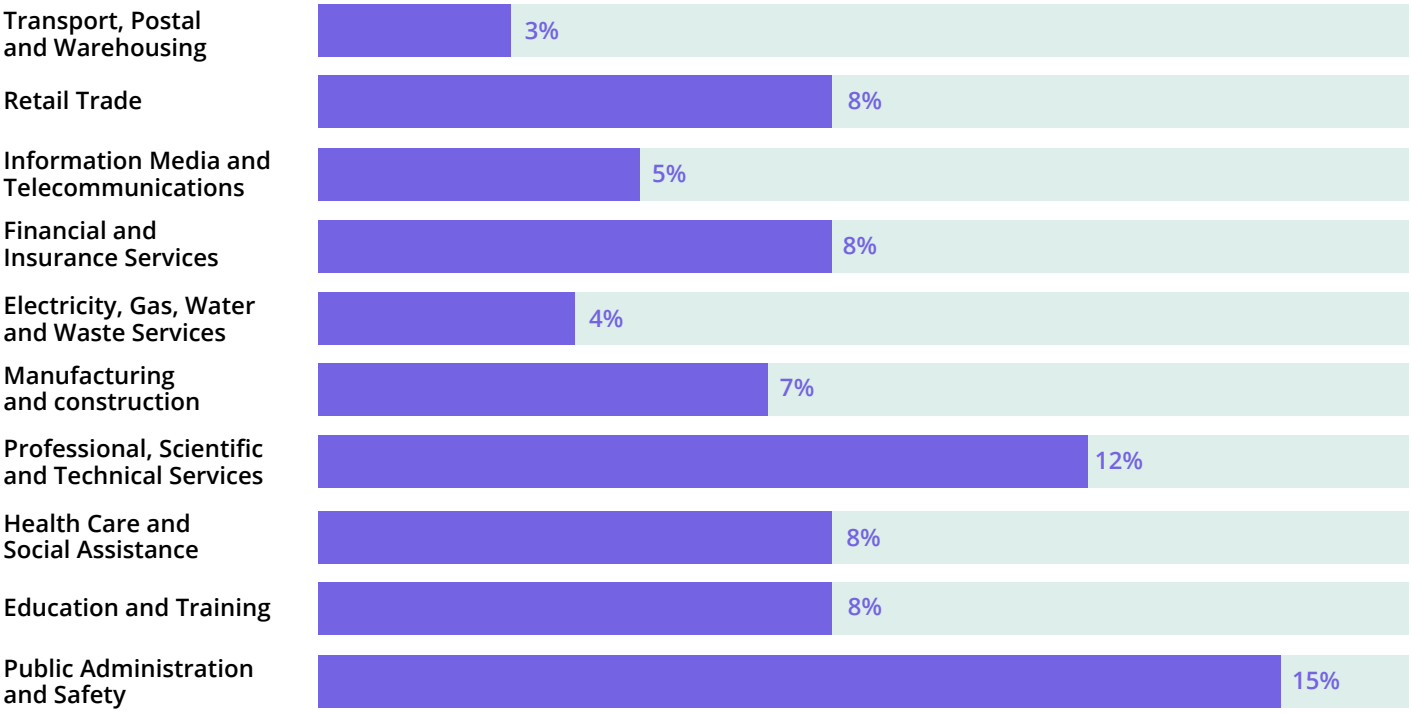
Of the remaining incidents, 162 indicated links to criminal or financially motivated actors, compared with 137 in the 2024/25 year.

The origin of 121 reported incidents could not be attributed.



BREAKDOWN BY SECTOR

The sectors most affected by incidents of potential national significance during 2025/26 were public administration and safety, health and social assistance and education and training. The public administration and safety sector, made up of central government agencies, local councils, public order and safety services, and defence, experienced a third of these potentially high-impact incidents. The NCSC also observed a doubling of attacks targeting the health care and social assistance sectors and education and training.



Glossary
Rarangi kupu

	TERM / KUPU	DEFINITION / WHAKAMĀRAMATANGA
A	**Advanced persistent threat (APT) / Tuma pakepake arā atu anō**	A well-resourced, highly skilled cyber actor or group that has the time, resources, and operational capability for long-term intrusion campaigns. Their goal is typically to covertly compromise a target, and they will persist until they are successful. They are very capable of compromising secured networks using both publicly disclosed and self-discovered vulnerabilities.
	Application Programming Interface (API) / He Tāhono Papatono	A set of rules and tools that allows software applications to communicate, share data, and request services from each other, enabling integration, automation, and functionality across different systems and platforms.
	Artificial Intelligence (AI) / Atamai Hangahanga (AI)	Computer systems which can perform tasks usually requiring human intelligence. See also Generative AI (GenAI) and Frontier AI.
B	**Botnet / Whatunga Pūwerewere**	Networks of compromised personal or office devices such as internet modems, personal computers, or network attached storage. Malicious cyber actors use these as infrastructure to send spam, perform denial-of-service activities, or attempt to obfuscate the origins of a malicious cyber campaign.
	Brute-force attack / He kōkiri takimano	A hacking method that systematically tries all possible passwords or encryption keys until the correct one is found, exploiting weak credentials through automated, repetitive guessing to gain unauthorised access to systems or data.
	Business Email Compromise (BEC) / He Whakamōrea Īmēra Pakihi	A cyber attack where criminals impersonate executives or trusted contacts via email to manipulate employees into transferring money, sharing sensitive data, or taking unauthorised actions, often leading to significant financial and operational consequences. BEC is a type of phishing attack.
C	**Cloud service / Ratonga kapua**	Provides ubiquitous, convenient, on-demand access to shared pools of computing resources such as servers, storage, or online applications.
	Common vulnerabilities and exposures (CVE) / Whakaraeraetanga	A vulnerability is a weakness in software, hardware, or a network that can be exploited by an actor. The Common Vulnerabilities and Exposures (CVE) database is a publicly available register of known vulnerabilities, each assigned a unique identifier in the format of CVE-yyyy-xxxx.
	Credentials / Whakatūturu pārongo	A user's authentication information used to verify identity – typically a password, token or certificate.
	Cryptocurrency miner / Maina moni whitirangi	Malicious software that co-opts computing resources for generating cryptocurrency. Many digital currencies require the solving of computationally intensive mathematical problems in order to generate digital assets.
	Cyberspace / Āteatāurungi	The global network of interdependent information technology infrastructures, telecommunication networks, and computer processing systems in which online communication takes place.

	TERM / KUPU	DEFINITION / WHAKAMĀRAMATANGA
C	**Cyber security /** **Whakahaumaru ā ipurangi**	Measures to protect systems, data and devices from unauthorised access and ensure the confidentiality, integrity, and availability of information.
D	**Data breach /** **Raraunga wāwāhi**	The intentional or unintentional release of sensitive or private information into an insecure environment.
	Defence evasion / **Karo kaupare**	A tactic that describes a series of attempts to prevent network defenders from discovering a malicious actor.
	Denial of service (DoS) / **Whakakore ratonga**	An attempt to make an online service unavailable by overwhelming the service with more traffic than it can handle.
	Disinformation / **Ngā kōrero horihori**	The deliberate, intentional spread of false and misleading information designed to achieve a strategic purpose.
E	**Endpoint /** **Pito Whakamutunga**	A network-connected device that acts as an access point for data and applications, including laptops, desktops, and mobile devices, often requiring security measures to prevent unauthorised access and cyber threats.
	Exfiltration / **Tāhae**	Where an actor has unauthorised access to private organisational data (for example, legitimate credentials or intellectual property) and copies it from a system.
F	**Frontier AI** **Frontier AI**	The most advanced and capable general purpose AI systems which can perform a wide variety of tasks and match or exceed the performance of today's most advanced systems.
G	**Generative AI (GenAI)** **AI Waihanga (Generative AI (Gen AI))**	A form of AI capable of generating new content, such as text, images or video in response to user prompts.
H	**Hacktivism /** **Porotū Mūrere**	The use of hacking techniques to promote political, social, or ideological causes, where activists breach or disrupt systems, leak data, or deface websites to draw attention to their message or protest perceived injustices.
	Hybrid threat / **Tuma momorua**	A mix of military, non-military, covert and overt activities by state- and non-state-sponsored actors that occur below the line of conventional warfare.
	Hypervisor / **Kaiwhakahaere pūrere mariko**	Software enabling the creation, management, and running of discretely hosted virtual machines (VMs) on the same hardware.
I	**Incident /** **Maiki**	An occurrence or activity that appears to have degraded the confidentiality, integrity, or availability of a data system or network.
	Indicators of compromise (IoCs) / **Paetohu whakamōrearea (ngā IoC)**	Usually IP addresses, domain names, or files that may be shared publicly or in confidence. Together they suggest a computer system or network may be compromised.
L	**Living off the land /** **He ora nō te whenua**	A technique using legitimate and pre-existing software on a victim network, in contrast to the installation of malicious software, to maintain network accesses. Use of legitimate software and accounts is less likely to raise alerts for defenders.

	TERM / KUPU	DEFINITION / WHAKAMĀRAMATANGA
M	**Malicious cyber actor /** **Nanakia tūkino mōhiohio**	An individual or group of people who seek to exploit computer systems to steal, destroy or degrade an organisation's information. Actors may be individual computer hackers, part of an organised criminal group, or state-sponsored.
	Malware / **Pūmanawa kino**	Malicious software or code intended to have an adverse impact on organisations' or individuals' data, such as viruses, Trojans, or worms.
	Mitigation / **Ārai mōrea**	Steps that organisations and individuals can take to minimise and address cyber security risks.
	MITRE ATT&CK framework / **Te Pou Tārawaho MITRE ATT&CK**	A knowledge base of adversary tactics, techniques, and procedures, used by cyber security professionals to understand, detect, and defend against cyber threats through structured analysis of attacker behaviour.
N	**Nationally significant organisation /** **Whakahaere hira ā-Motu**	Organisations such as government agencies, key economic generators, niche exporters, research institutions, and operators of critical national infrastructure. If these organisations were affected by a cyber security incident, the impact could lead to national-level harm.
	Network-attached Storage (NAS) / **Rokiroki Āpiti-Whatunga**	A dedicated device connected to a network that provides centralised file storage and sharing for multiple users or systems.
O	**Operational Technology (OT) /** **He Hangarau Whakahaere**	The systems and equipment used to control, monitor and manage industrial processes and physical operations, such as machinery, power grids, and transport systems, enabling real-time automation and safety in critical infrastructure.
	Opportunistic cyber activity / **Ngohe ā-ipurangi tūpono**	Occurs when malicious cyber actors select their victims based on the availability of a vector of compromise, regardless of victim location, sector or intelligence value.
P	**Personal information /** **Ngā mōhiohio whaiaro**	Information about an individual, including name, date of birth, biometric records, medical, educational, financial, and employment information.
	Phishing / **Hītinihanga**	The use of fake, deceptive or alluring messages to solicit a behaviour from the recipient – such as clicking a link or divulging personal information or credentials.
	Public attribution / **Whakahuatia whānuitia nō hea**	A tool used by governments and private-sector organisations to deliberately release information about the source of a cyber intrusion, primarily to uphold norms about what constitutes acceptable state behaviour in cyberspace.
R	**Ransomware /** **Pūmanawa utu uruhi**	A type of malware designed to disrupt the use of computer systems and files until a ransom is paid.
	Ransomware-as-a-Service (RaaS) / **Ko te taupānga-whawhe-hei-ratonga**	A criminal business model where developers sell or lease ransomware tools to affiliates, who deploy attacks and share profits. It lowers technical barriers, enabling widespread, scalable cyber extortion campaigns.
	Reconnaissance / **(TE REO)**	Intelligence gathering by malicious actors of your business, its people and systems. This capability can be used to develop personalised attacks on individuals and identify weaknesses in your systems.

	TERM / KUPU	DEFINITION / WHAKAMĀRAMATANGA
S	**Small Office/Home Office (SOHO) / Tari Iti / Tari Kāinga**	A business setup with few employees operating from a small or home-based workspace, using consumer-grade technology to manage professional tasks, communications, and network operations.
	Social Engineering (TE REO)	The manipulation of individuals to access networks and systems using persuasive techniques including deepfakes, impersonation and personalised messages.
	Spear phishing / He hītinihanga ā-tao	A targeted cyber attack where malicious actors craft personalised messages to trick specific individuals into revealing sensitive information, clicking malicious links, or installing malware, often by impersonating trusted contacts or organisations.
	Supply chain compromise / Poke ara ratonga	A form of attack that targets software, hardware or an IT service provider, where the ultimate aim is to exploit downstream customers.
T	**Targeted cyber activity / Ngohe ā-ipurangi heipū**	Occurs when malicious cyber actors demonstrate an intent or a tasking to compromise an organisation for its intelligence value, regardless of a specific access vector.
V	**Virtual Private Network (VPN) / Whatunga Tūmataiti Mariko**	A secure connection that encrypts internet traffic and routes it through a remote server, protecting user privacy, hiding IP addresses, and helping to prevent data from being intercepted on public or untrusted networks.
	Virtual private server (VPS) / Tūmau tūmataiti mariko	A portion of a large physical server divided into virtual spaces available for temporary use.
Z	**Zero-day vulnerability / Whakaraeraetanga rā-kore**	A software vulnerability for which there is currently no patch, and for which there is often no CVE number assigned. The term derives from the number of days for which defenders and developers have been aware of the vulnerability.

Te Tira Tiaki
Government Communications
Security Bureau