New Zealand's Cyber Security Strategy

2026–2030

Embracing cyber security to enable innovation, drive a prosperous economy and protect our digital way of life.

FEBRUARY 2026 | CYBERSTRATEGY@DPMC.GOVT.NZ

Te Kāwanatanga o Aotearoa
New Zealand Government

For more information on the work of the Department of the Prime Minister and Cabinet (DPMC),
please visit our website dpmc.govt.nz

ISBN 978-1-0670255-5-7 DIGITAL

Contents

Ministerial foreword

Digital technologies underpin nearly every aspect of our lives and have provided our society and economy with unprecedented opportunities for connection and growth. This connectivity, however, exposes New Zealand to an ever-rising tide of malicious cyber activity.

All New Zealanders need to be able to engage with digital services knowing their data and privacy are protected. New Zealand businesses need to be able to innovate and trade with confidence and our critical infrastructure needs to be resilient.

As outlined in New Zealand's National Security Strategy, security is the foundation of our prosperity, and adopting a whole-of-society approach is how we build strong foundations.

In the past, New Zealand's geographic isolation has provided a sense of protection from global security threats, but this is no longer the case. Threats to New Zealand are becoming increasingly borderless, and this is especially true in the cyber domain.

Recognising this, New Zealand's Cyber Security Strategy is designed to foster collaboration between government, industry, and community stakeholders. It also sets out our intention to work with our international partners, to strengthen our collective capacity to respond to, and recover from, cyber threats.

The rapidly evolving and increasingly damaging nature of cyber threats underscores the vital need for a proactive and multi-faceted cyber security strategy. This strategy has a focus on a commitment to defence and resilience at all levels of the economy, as well as a commitment to promoting the international rules and norms that underpin a free, open and secure cyberspace.

These challenges also affect our partners in our Pacific neighbourhood and this strategy supports our commitments under the Boe Declaration on Regional Security to work towards a more resilient Pacific.

This strategy outlines a clear vision and actionable roadmap to secure our digital domain, highlighting cyber security not just as a defensive measure, but a critical enabler of economic growth and future competitiveness.

Rt Hon Christopher Luxon
Minister for National Security and Intelligence

Cyber security outlook

The cyber threat to New Zealand is a significant national security challenge.

The ubiquity of information technology across all sectors, from public services, critical infrastructure, in the private sector and the everyday lives of citizens, provides a wide surface area for malicious cyber actors to target New Zealand.

Malicious actors use cyber means to conduct a broad range of activity that can harm New Zealand's national interests and security. This includes ransomware attacks and cyber extortion, espionage and foreign interference, activities that seek to undermine the integrity of our democracy, the theft of sensitive intellectual property, and disruptive attacks against critical infrastructure.

The current geostrategic environment is complex. Ongoing conflict and competition continues to place pressure on the international rules and norms that protect the security and stability of cyberspace. New Zealand's place and role in the Indo-Pacific – a strategically important region – means our exposure to national security threats, including those that manifest in the cyber domain, are becoming more acute.

PARLIAMENTARY NETWORK BREACH

In 2021, a malicious cyber actor compromised the networks of the Parliamentary Counsel Office and the Parliamentary Service. The intrusion, investigated under the code name 'Operation DUSKGLOW', was attributed by the NCSC to APT40, a threat actor affiliated with the People's Republic of China's (PRC) Ministry of State Security. In March 2024, the New Zealand Government publicly called out the PRC's actions, in line with our commitment to responding to malicious cyber activity that we believe harms our interests and national security.

New Zealand's National Security Strategy, released in 2023, sets out cyber security as a core national security issue that requires a proactive, coordinated response. The National Security Strategy also recognises that the complexity of our strategic context requires a concerted effort from government to foster robust, open dialogue with the New Zealand public about the kinds of national security threats that our country faces, including cyber threats.

Cyber security is a key concern for many New Zealanders. In a 2024 survey, the public rated cyber threats as one of the top five national security issues facing New Zealand, with 62% of New Zealanders wanting to receive more information about these threats and how government is responding.

These concerns are well-founded. Cyber threats directly affect the livelihoods of New Zealanders and their communities. New Zealand has seen a significant increase in the level of cybercrime in recent years. It is estimated New Zealanders are losing more than $1.6 billion annually to cybercrime, mainly in the form of cyber-enabled fraud. In a survey of 295 large New Zealand businesses, 59% reported experiencing a cyber incident in the last year. Without decisive action, these costs and the frequency of incidents will continue to increase, impacting business operations, reputation, and bottom line.

As we look to the global outlook in 2030, four interlinked drivers inform our strategy.

Changes in technology continue to challenge cyber security

Artificial Intelligence (AI) has become a common tool for those seeking to defend networks and those seeking to harm others online. Machine learning and other AI tools can assist defenders in analysing high volumes of data and automating mundane tasks. Generative AI has also allowed creation of more realistic phishing emails in multiple languages. Software and hardware innovations continue to change the way people use digital systems, with the speed and scale of computational systems having vastly increased. Within the timeframe of this strategy, quantum computing has the potential to render current encryption methods obsolete and turn today's secure communications into tomorrow's open books. Technological change is not just incremental; it is transformative.

Malicious cyber activity and technology development are increasingly part of strategic competition

Malicious cyber activity is becoming integral to broader global campaigns of malign behaviour, as demonstrated by the attack on international satellite infrastructure by Russia, as part of its illegal invasion of Ukraine. These geopolitical issues are reaching into our own Pacific neighbourhood, including through cyber-enabled espionage and state-sponsored attacks affecting the critical systems that keep our economies and communities functioning. State actors are also increasingly using social media platforms as tools to amplify the reach and impact of information campaigns for strategic influence and to undermine democratic processes.

Our digital supply chains have grown more interconnected and more frequently targeted

Digital supply chains are integrated and complex, creating new points of strategic risk. Technical debt and legacy systems often form the 'weak links in the chain', with many systems operating with limited security protections.
We rely on a complex and opaque technology supply chain, which includes critical components like semiconductors, open-source software and a vast range of technology vendors, including some that present jurisdictional risks. Within these supply chains, sensitive New Zealand data from businesses and individuals traverse the digital ecosystem with limited visibility and assurance around mitigating critical risks. As malicious actors increasingly target the points of vulnerability in these supply chains, protecting our critical infrastructure and services has become a task requiring security at every level in the digital supply chain.

CROWDSTRIKE OUTAGE

In July 2024, a CrowdStrike software update caused a widespread IT outage for some Microsoft customers, leading to system disruptions across various sectors including healthcare, airlines, and emergency services. New Zealanders reported queues at supermarkets due to checkouts going down, disruption at Christchurch Airport and commuters being unable to tag on or tag off with Auckland Transport HOP cards. While not a result of malicious activity, the incident highlighted our reliance on the digital supply chain, with an error made by one company imposing at least $5.4 billion of costs to businesses globally.

The number and capability of threat actors is growing

The ecosystem of malicious actors has become more diversified, professional and, in many cases, blurred in the division between state and non-state actors. Cybercriminals have created a black market, where affordable and sophisticated digital tools, support, and expertise are traded. Malicious actors of all types can easily access expertise and infrastructure to steal highly sensitive data and perpetrate devastating cyber attacks.

Criminal ventures often operate out of jurisdictions that allow them to act with impunity, enabling them to financially exploit New Zealand businesses and citizens with ransomware or other forms of cyber extortion. Scams and other financial crimes are being undertaken on an industrial scale. While cybercriminals continue to innovate and adopt advanced techniques, they will still take advantage of those who get the cyber security basics wrong.

Basic failures to protect login credentials, patch software, and configure systems correctly, continue to be the starting point for many cybercrimes. We must continue to be vigilant by building awareness and minimising poor cyber security practices that leave our front doors open and unguarded.

CYBER INCIDENTS IN THE HEALTH SECTOR

In May 2021, the Waikato District Health Board suffered a significant ransomware attack that severely disrupted its services and compromised its systems. The attackers cut off access to a range of clinical and administrative data which resulted in cancellations or delays of patient appointments and surgeries. Critical communication systems, such as phone access, were also taken offline. The incident threatened the lives of patients and demonstrated the intent of threat actors to enrich themselves at the expense of the most vulnerable members of our community. The Waikato District Health Board did not pay the ransom and restored its systems.

In December 2025, attackers gained unauthorised access to sensitive personal information on Manage My Health, and made extortion demands. Around 100,000 patients had records stolen.

Building a cyber secure and resilient New Zealand

A strategy for strengthening foundations and protecting New Zealand's cyber security out to 2030.

Cyber security is every person's responsibility. In recent years, New Zealand's awareness of cyber risks, and the importance of secure practices and reporting has undoubtedly increased with the rapid adoption of digital technologies.

The National Cyber Security Centre (NCSC) provides guidance for individuals through to critical infrastructure providers. The advice available to all New Zealanders includes online security assessment tools, guides and alerts to help protect themselves, and a range of technical resources for large organisations. To prevent cyber threats from reaching New Zealand homes and businesses, the NCSC's Malware Free Networks (MFN) service disrupts threats and helps businesses to target their limited resources efficiently, building collaboration and trust across industry partners.

However, cyber threats continue to outpace our collective response, while the sophistication and adaptability of malicious cyber actors continues to challenge defence and detection capabilities nationwide.

New Zealand's Cyber Security Strategy 2026–2030 will better position New Zealand to respond to our most strategic cyber threats. A key priority is to strengthen the cyber security of New Zealand's critical infrastructure system so it can continue to provide the services that New Zealanders rely on every day. It also includes ensuring the adoption of higher and more consistent security and ICT procurement standards across government. Our legislation, threat detection capabilities, and international engagement settings must all be updated to keep pace with modern threats.

To realise our vision, New Zealand will be strengthening the solid foundations that have already been built by previous cyber security strategies. The strategy comprises four key objectives that will guide our efforts: Understand, Prevent and Prepare, Respond, and Partner.

An Action Plan for 2026–2027 details immediate, first steps to realise the strategy's objectives. However, these actions alone will not suffice to manage cyber risks, uplift our cyber capability and build our national cyber resilience. We will therefore deliver the strategy in phases, reviewing our progress and refreshing the Action Plan regularly to better protect New Zealanders and New Zealand businesses against cyber threats.

LEADING BY EXAMPLE

In April 2023, New Zealand became one of the first countries in the world to impose a ban on ransomware payments by government agencies. This position recognises that paying a ransom fuels the ransomware business model, making New Zealand less safe in the future. The government continues to discourage the payment of ransoms by New Zealand businesses and individuals and will provide support and guidance to those affected by ransomware attacks.

2024/25, NCSC disrupted over

473.4 MILLION

MALICIOUS CYBER EVENTS VIA MALWARE FREE NETWORKS®

COMPARED TO 10.3 MILLION IN 2023/24

Continuing a pattern of exponential growth

145,000+

UNIQUE INDICATORS

published since 2021 (as at March 2025)

59% OF BUSINESSES EXPERIENCED A CYBER INCIDENT

in the past 12 months

1 IN 6 SAW PERSONAL INFORMATION ACCESSED OR STOLEN

KORDIA // NZ BUSINESS CYBER SECURITY REPORT 2025

1.4% PROSPECTIVE DROP IN GDP

from a potential cyber attack on the Auckland electricity system

NZIER // CGE MODELLING 2023

331 INCIDENTS TRIAGED

for specialist technical support because of potential national significance

COMPARED TO 343 INCIDENTS IN 2023/2024

25% INCIDENTS (82/331)

of potential national significance

indicated links to suspected state-sponsored actors

COMPARED TO 32% IN 2023/2024

NCSC // CYBER THREAT REPORT 2025

83% of NZers considered that HACKING INTO INFO SYSTEMS WAS LIKELY TO BE A THREAT

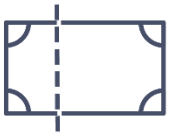
in the next 12 months

IPSOS // NATIONAL RISKS PUBLIC SURVEY 2024

Likely over –

$1.6 BILLION IN DIRECT LOSSES

from online threats annually in NZ



NCSC // ESTIMATE 2025

Our vision

New Zealanders embrace cyber security to enable innovation, drive a prosperous economy and protect our digital way of life.

Our objectives on the path to 2030 are to:

 **UNDERSTAND**	 **PREVENT & PREPARE**	 **RESPOND**	 **PARTNER**
We are well aware of cyber risks and know how to protect ourselves	We manage cyber risks to prevent harm and are well-prepared when incidents occur	We react effectively and decisively to adverse cyber incidents	Our resilience to cyber threats is bolstered by strategic and targeted cooperation
By 2030 the outcomes we want to achieve are:			
• Government and industry share information to better understand and navigate the evolving threat environment. • More New Zealanders and organisations are aware of practical steps to improve their cyber security and are supported to take action. • It is easy to report cyber incidents and cybercrime, and to access practical support. • The development and use of emerging technologies is safe and secure.	• Government and industry have adopted good cyber security practices and have arrangements in place to respond to cyber risks. • New Zealand's legislation is fit-for-purpose to manage cyber threats. • New Zealand's most sensitive information is protected against evolving cyber threats. • Government and industry are well-prepared to respond to significant cyber incidents. • Good cyber security is built into the digital supply chain.	• Government's capability to detect and disrupt high impact threats, including cybercrime, is fit-for-purpose. • Victims are supported to be better able to remediate, recover and bounce forward from cyber incidents and cybercrime. • New Zealand's legislation is fit-for-purpose.	• New Zealand is a trusted partner and engages actively in global efforts to protect the stability of cyberspace. • New Zealand's cyber security posture is lifted through stronger collaboration between government and industry. • Our Pacific partners are supported to build cyber capability and resilience.

Objective 1: **Understand**

We are well aware of cyber risks and know how to protect ourselves.

We need to take action

In an environment where 91% of New Zealanders go online at least several times a day, cyber risks are not just a possibility; they are an almost certain part of our everyday life. This applies to everyone from home users through to the operators of critical infrastructure.

A 2024 survey commissioned by the NCSC highlighted the challenges we face. Many New Zealanders are increasingly complacent about their cyber security knowledge. While more than half consider their cyber security knowledge intermediate or advanced, basic steps such as password hygiene continue to be ignored. Businesses also face similar challenges. A 2025 survey by Datacom found that many businesses overestimate their resilience and ability to handle cyber threats, with a clear divide between business leadership and staff member assessments of awareness and preparedness.

Currently, the fragmented nature of cyber incident reporting mechanisms across government discourages individuals and businesses to report, making it challenging to provide the public with a comprehensive picture of the threats we face. Without consistent and complete reporting of cyber incidents, the risk of complacency will grow and leave us exposed to more serious cyber incidents in the future.

Immediate steps to build capability

The NCSC will establish a single cyber security reporting service that enables NCSC to receive, respond to and manage cyber incidents. Processes will be established for other types of online harm and cyber-enabled crime to be redirected to appropriate agencies.

Alongside improved reporting, the government will continue information exchanges with industry. Ongoing dialogue and partnerships with industry will help defend against immediate threats and coordinate our approaches to emerging challenges.

The government will also support critical infrastructure owners and operators by providing tailored guidance on cyber risk. It is imperative that the entities responsible for our essential services have the most comprehensive and practical advice at their disposal to protect against digital disruption. This focused guidance will include assessments, strategies for risk management, and guidance to implement technical controls to protect IT and OT networks. This guidance and best practice information will closely align the New Zealand market with international partners, including Australia, and foster business connections between nations.

Objective 2: **Prevent and prepare**

We manage cyber risks to prevent harm and are well-prepared when incidents occur.

We need to take action

Malicious actors are constantly seeking to take advantage of any vulnerability in our networks and systems. While it is critical that we seek to prevent malicious cyber activity, we must also prepare for when things go wrong, to minimise the impact. Often, we will be affected by incidents that we cannot control.

Disruptions to critical infrastructure assets, systems, and networks have a debilitating effect on national security, economic performance, public health, and safety. While the higher risk profile of critical infrastructure is well known, many entities have not consistently managed cyber risk to align with leading practice. Many countries have taken a regulatory approach, with approximately 120 countries globally having some form of critical infrastructure regulation. Improving the cyber resilience of our critical infrastructure will not only protect existing assets and the services they provide but also act as a strategic investment in the country's future resilience, investment attractiveness and economic growth.

As another provider of critical services, government must also address security vulnerabilities within its agencies that pose an unacceptable risk to networks on which the public relies. Duplications and inefficiencies that stand in the way of improving security must be eliminated. Government agencies must also be empowered to invest in the capability needed to adapt our detection and disruption capabilities to changes in cyber threats and technologies. Getting the strategic settings in government right can have a positive ripple effect through the economy.

Immediate steps to build capability

The government will take several actions to ensure that agencies are coordinated and empowered to respond to cyber risk. We will strengthen the existing mandate for the Government Chief Digital Officer (GCDO) to entrench a culture of security that starts from procurement through to system operations, with support from the Government Chief Information Security Officer (GCISO).

The GCISO will continue to establish and enforce minimum cyber security standards and work with digital supply chain vendors to apply more consistent security controls across agencies. The GCSB will also refresh its Cryptographic Products Management Infrastructure to ensure government ICT will be prepared for the emerging needs of a post-quantum world. The GCDO is now empowered to take a more directive approach to digital governance and strengthen the management of ICT procurement.

Beyond government, we will ensure that New Zealanders can rely on the continuity and security of critical infrastructure services by developing a regulatory regime to improve the cyber security of critical infrastructure. As a first step, the government will consult industry and the public on the core elements of a regulatory framework, including additional non-regulatory actions the government can take to better partner and support critical infrastructure owners and operators to manage cyber risk.

We will also work to raise the standard of data security in New Zealand, including exploring the development of options to ensure organisations or businesses that hold personal information adopt adequate protections.

Objective 3: **Respond**

We react effectively and decisively to adverse cyber incidents.

We need to take action

Cyber incidents are, and will continue to be, an unavoidable part of our interactions online, with consequences that extend well beyond the immediate technical disruptions. As with all types of business disruptions, time is money and the longer an incident goes unresolved, the greater the cost for businesses and individuals to recover. When critical public systems or national infrastructure are compromised, the costs can spread across the economy, with disruptions to essential services potentially leading to substantial impacts.

Responding is not just technical, it is about people and how we help them recover. Victims of cyber incidents expect the government to play an important role in providing support to resolve incidents quickly and help businesses and individuals to bounce back stronger. However, government agencies face legislative barriers to better support businesses and individuals to respond to incidents. This includes limitations in search and surveillance powers, capacity to share information and access evidence from international partners and authority to disrupt threat actors online. Effective responses also rely on regular exercises to test and maintain readiness.

New Zealand's role as a globally engaged democratic country, with niche strengths in innovation and research, is of interest to foreign states. State-sponsored cyber actors continue to demonstrate the intent and capability to target New Zealand's networks, and it is important that we are able to effectively respond to and deter activity that is designed to hurt our national interests.

Immediate steps to build capability

Under this strategy, victims of cyber security incidents, including cybercrime, will be supported to remediate and recover. We will take steps to limit the harm to victims when their personal information is stolen by cybercriminals. The government will work to ensure that New Zealand has the response options needed to effectively deter malicious cyber activity and impose costs on those who seek to do us harm. Key to this will be modernising our legislative frameworks to account for the complexity and global nature of the cyber threat. Government will work to address jurisdictional barriers so that New Zealand law enforcement agencies can access digital evidence to effectively investigate cybercrime. Over the life of the strategy Government will continue to assess whether our laws remain relevant to the modern technology environment.

The Government will continue to evolve its capability to detect and disrupt high impact threats, including cybercrime. Immediate steps include our response to the review of the Intelligence and Security Act 2017, which will consider the powers and capabilities of our intelligence and security agencies to proactively disrupt a broader range of cyber threats. These reforms will ensure that our agencies have the legislative powers to respond to adversaries and protect our national interests. The New Zealand Government will continue to work closely with likeminded international partners to respond to and deter malicious state-sponsored cyber activity. When it is in our national interest, this will include public attribution of significant cyber incidents and calling out activity that runs counter to the internationally agreed framework for responsible state behaviour in cyberspace.

Objective 4: **Partner**

Our resilience to cyber threats is bolstered by strategic and targeted cooperation.

We need to take action

Geostrategic competition is continuing to make New Zealand less safe and secure, including in the cyber domain. Cyber threats are inherently cross-border, meaning all countries are vulnerable to the risks posed by the increasing pace, scale, and impact of cyber attacks. Industry partners, working across a global digital economy and multiple jurisdictions, face the same challenge.

Cooperation with our international partners and industry community is a critical enabler of domestic cyber resilience and a means of promoting New Zealand's interests in a free, open, secure and global internet. Through our partnerships, we can share best practice, disrupt and deter malicious cyber activity such as cybercrime, and promote our values and interests online. For example, our membership of the international Counter Ransomware Initiative helps collectively build resilience against ransomware attacks. There are, however, several barriers to partnership that need to be resolved to ensure that we can share information freely and quickly enough to take action against cyber threats.

Immediate steps to build capability

New Zealand's international relationships enable us to better defend our networks from harm. Engaging with international partners offers us opportunities to share information about emerging threats, improve our policy settings and operational capabilities to respond to threats. They also help deliver coordinated and complementary support in the Pacific, and cooperate across borders to ensure no cybercriminal can hide from the law.

In response to increasing destabilisation in cyberspace, characterised by global conflict and competition, New Zealand will take a proactive approach to promoting and defending our interests and values in international fora.
In line with our commitment to upholding the international rules-based order, New Zealand will continue to contribute to discussions that shape the international rules, norms, and standards that underpin cyberspace. We will continue to advocate for the inclusion of industry, civil society, and other non-government stakeholders in global discussions, which we see as critical for the development of practical, human rights-respecting, and technically viable solutions to global cyber security challenges.

Our National Security Strategy underscores our national interests in enabling and promoting a peaceful, stable, prosperous, and resilient Pacific region. New Zealand will continue to work with our Pacific partners toward greater collective cyber resilience, so that our region can prosper through digital transformation. This includes supporting cyber security uplift through targeted, meaningful, and sustainable capacity building initiatives that enable our partners to protect the data and systems that their people rely on.

Close collaboration with industry will be critical for our ongoing ability to understand and respond to evolving cyber threats. Sharing unique insights and threat intelligence with private sector partners gives us a clearer picture of the cyber threats in New Zealand and how global trends are impacting us. This additional information can inform the government's policy and operational priorities and enable agencies to act early to respond to and disrupt threats before they cause significant harm to New Zealand.

Glossary

Boe Declaration

In 2018 Pacific Islands Forum leaders agreed the Boe Declaration on Regional Security, which responds to a more complex environment with an expanded concept of security, including cyber security, and calls for closer coordination in the Pacific region.

Critical infrastructure

The assets, information, networks, systems, suppliers, people and processes providing essential services that, if disrupted, would have national or otherwise significant and/or widespread consequences for public order, public safety, public health, national security or the functioning of the economy.

Cyber incident – cyber security incident

An event, whether intentional or not, that causes adverse consequences to an ICT system or its data.

Cyber resilience

The ability to anticipate, withstand, recover from, and adapt to cyber incidents and attacks.

Cyber security

Protecting people and their computers, networks, programs and data from cyber attacks.

Cybercrime

Crimes that are committed through the use of computer systems and are directed at computer systems. Examples include producing malicious software, denial of service attacks, and phishing.

Cyber-enabled crime

Crimes that are assisted, facilitated or escalated in scale by the use of technology. Examples are online scams and fraud and the online distribution of child exploitation material.

Cyberspace

The internet and everything connected to it – the global network of interdependent information systems, telecommunications networks and systems with embedded ICT.

GCDO

The Government Chief Digital Officer sets the direction and is responsible for driving a unified approach to digital government for New Zealand.

GCISO

The Government Chief Information Security Officer sets foundational information security controls for information held within ICT systems that government departments must follow and use, and performance controls to support prioritisation of digital investment, to lift information security across government.

Information Technology/Information and Communications Technology (ICT)

Technologies and equipment that handle (e.g. access, create, collect, store, transmit, receive, disseminate) information and communication, associated devices, services and applications and their governance.

Operational Technology (OT)

The range of programmable systems and devices that manage or control physical systems and equipment. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems.

Ransomware

A type of malicious software that locks up the files on an information system until a ransom is paid.