National Cyber Security Centre

Strategy to 2024

Every day, we protect New Zealand and its interests.

Te Tira Tiaki
Government Communications Security Bureau

Foreword

I am pleased to share the National Cyber Security Centre (NCSC) strategy to 2024. The NCSC supports nationally significant organisations to improve their cyber security, and we respond to national-level harm and advanced threats. This strategy outlines our mission, objectives and offerings in service of this purpose.

Making the NCSC's strategy publicly available makes our work more accessible. Our people work at the heart of New Zealand's cyber defence. We are proud of the part we play in enabling our country's protection, wellbeing and prosperity as we work towards a safer digital world for Aotearoa New Zealand.

Our strategy to 2024 was initially generated to reflect new Budget 2020 investment. Cyber security is a rapidly evolving domain. In reviewing our strategy for publication, we have taken the opportunity to incorporate updates. These enable us to recognise achievements and challenges. They respond to new perspectives, strategies, requirements, and further investment. They allow us to adapt to our changing role in New Zealand and the global technology environment.

Two years in to our four-year strategy, we are making meaningful progress. We have delivered a major uplift in national threat detection and disruption with the launch of Malware Free Networks.

Establishing the Government Chief Information Security Officer (GCISO) role has focused us on systemic public sector issues like secure cloud adoption and investment decision criteria.

We have also completed a nine-year project to replace New Zealand's high-grade encryption system with a modern, scalable, cryptographic infrastructure that protects the Government's classified communications.

We have responded to high-profile cyber incidents including the Waikato DHB and New Zealand stock exchange, and we provided proactive support to major events such as the COVID-19 vaccine rollout and 2020 General Election.

As the security environment changes, we must adapt our approach in response. Increasingly, we work at scale. This means greater collaboration to secure key digital supply chains, through technical and policy avenues. We are building relationships to achieve greater national resilience together than we could alone. We seek to pair our knowledge with others to improve the value and impact of our respective work.

Our strategy to 2024 reflects the reality that effective response in today's cyber threat environment requires a team approach in which we work closely with domestic and international partners. We expect to keep updating our approach as our environment changes and our service offering continues to adapt.

Lisa Fong (she/her) *Deputy Director-General, National Cyber Security Centre*

Our mission

We protect Aotearoa New Zealand's wellbeing and prosperity through trusted cyber security services.

Our objectives

This strategy establishes three outcomes to pursue for New Zealand:

Defend National Security

New Zealand's values and way of life are protected, and New Zealand's information security culture is globally respected and trusted.

Raise Cyber Resilience

New Zealand's digital environment is able to withstand adversity, and organisations play an active role in protecting themselves.

Facilitate Digital Transformation

New Zealand organisations embrace technology responsibly and securely.

Our Strategy

Relationship with other security strategies

This document provides the NCSC's strategic vision for information assurance and cyber security in New Zealand. It aligns with the broader GCSB and New Zealand Intelligence Community strategic outcomes, the New Zealand Cyber Security Strategy (2019-2023), the Digital Strategy for Aotearoa, and the strategy for a digital public service.

Strategic context

The digital world has removed borders and transformed the ways in which public and private-sector organisations operate. Being connected online is now essential in creating new opportunities for New Zealand to grow and prosper.

As we move towards a more digital economy, an increasing amount of data is being stored online by individuals, private organisations and government agencies and operations are more dependent on digital supply chains.

The geopolitical picture has shifted as a result of new technologies, adversaries becoming more tech savvy, and a greater range of threat actors making the most of cyber-enabled tools to steal information and launch attacks. Alongside the increase in malicious activity is a limited awareness of the impact and importance of information security practices.

Cyber security is important for all New Zealanders. Although we are focused on the cyber resilience of nationally significant organisations and responding to national-level harms, we recognise that our work has wider impact and we continue to find ways to scale our efforts through collaboration and partnerships.

NCSC Strategy at a glance

Our mission

We protect Aotearoa New Zealand's wellbeing and prosperity through trusted cyber security services.

Our objectives

Defend National Security | Raise Cyber Resilience | Facilitate Digital Transformation

Our services

Detect: We alert our customers to malicious activity, threats and vulnerabilities.

Disrupt: We prevent threats from harming our customers.

Advise: We guide and equip our customers to protect their valuable information and manage risk.

Deter: We raise the cost for our adversaries in targeting New Zealand.

What we do to protect Aotearoa New Zealand's wellbeing and prosperity.

Our objectives

This strategy establishes three objectives to pursue for New Zealand:

Defend National Security

New Zealand's values and way of life are protected, and New Zealand's information security culture is globally respected and trusted.

Why is it important?

Defending New Zealand's national security is a fundamental part of the success of this strategy. Information security threats have evolved significantly over the last few years and continue to develop with advancing technologies. We play a crucial role in upholding New Zealand's way of life and global standing by maintaining trusted and effective information security protections at a national level.

Raise Cyber Resilience

New Zealand's digital environment can withstand adversity, and organisations play an active role in protecting themselves.

Why is it important?

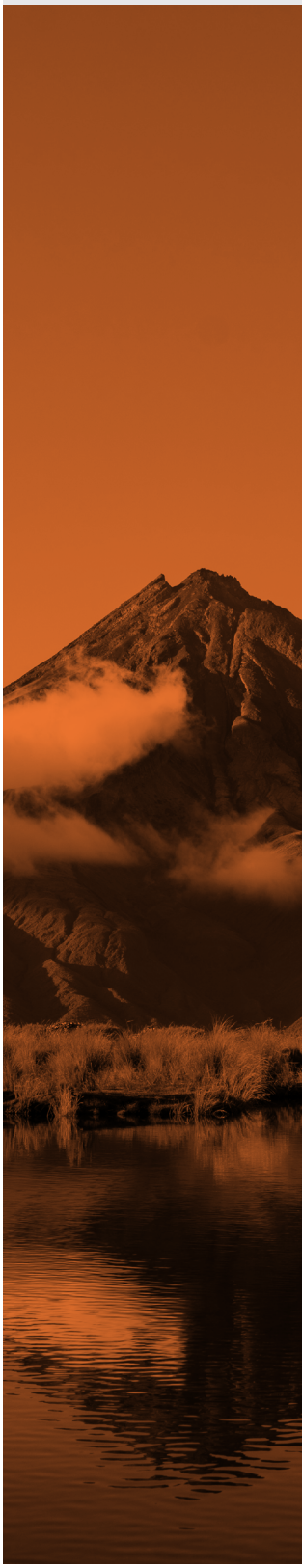
New Zealand has an opportunity to be a world leader in the information and cyber security space. To achieve this, nationally significant organisations will play active roles in reducing their cyber security risk, ensuring their systems and information are safe and secure, and by role-modelling good practice across the wider economy.

Facilitate Digital Transformation

New Zealand organisations embrace technology responsibly and securely.

Why is it important?

Digital transformation provides the foundation for New Zealand organisations to flourish. As organisations continue to expand their digital footprints, the information security risks associated with digital business are increasing in parallel. It is important to embed security solutions and processes into business to secure vital assets and mitigate any risks.



How we protect Aotearoa New Zealand's wellbeing and prosperity.

Our services

We provide a wide range of services to keep our country and our nationally significant customers safe.

DETECT

Cyber threat detection & reporting | Incident reporting | Assurance reporting

We detect indications of malicious activity or vulnerabilities and provide timely and evidence-based advice to our customers on best-practice techniques to mitigate potential risks to their operating environments.

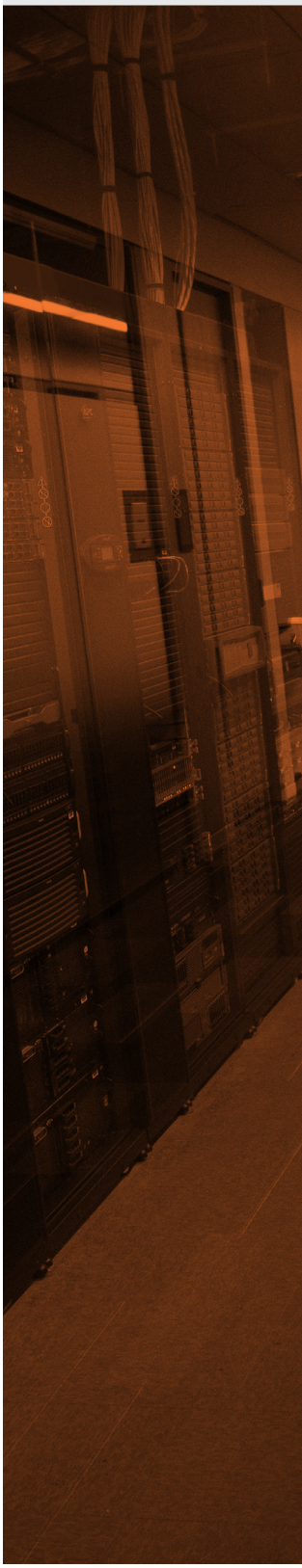
- **We protect New Zealand's information networks** by deploying our cyber security technologies to detect and discover cyber threats.
- **We ensure the New Zealand Government's classified systems are free from compromise** by providing inspection activities, including assurance to SCI systems, sites and diplomatic posts.
- **We support evidence-based decisions** by providing cyber threat and intelligence reporting and advice to key public and private-sector customers.
- **We measure resilience** across our customers to understand where we need to focus our efforts.

DISRUPT

Active disruption | Incident management | Mitigation advice

We prevent threats from harming our customers' environments by providing best-practice mitigation advice and, when required, intervening to remove and dispose of threats.

- **We provide protection for our customers** by blocking harmful activities through our active disruption capabilities.
- **We support our customers' incident response activities** by isolating and removing potential threats or vulnerabilities from their environments.
- **We support our customers to protect themselves** by advising them on potential threats within their landscape and providing advice on how to mitigate them.



ADVISE

INFOSEC standards & policy | INFOSEC advice & guidance | Regulatory oversight | Intelligence reporting & briefings

We guide and equip our customers to protect their valuable information and manage risks. We act as trusted, independent advisors, reducing the cost across the system by providing assurance, mitigating risk, enabling innovation, and supporting our customers through security issues.

- **We improve New Zealand's information security maturity** by developing, managing and promulgating policies, standards and guidance.
- **We improve New Zealand's security resilience** by working with government agencies and nationally significant organisations.
- **We support decision-making advantage** by informing national security determinations with fit-for-purpose reports and briefings.
- **We provide system leadership for the Government** through our work in support of the Government Chief Information Security Officer.

DETER

Cryptographic product support | Inspection & accreditation | Regulatory framework | Cyber threat attribution

We raise the cost for our adversaries in targeting New Zealand by providing best-practice and world-leading information security services.

- **We ensure the confidentiality and integrity** of the New Zealand Government's classified information and communications by providing high-grade encryption capabilities.
- **We ensure the safety and security** of the New Zealand's Government's most sensitive information through regular inspections and accreditation of classified sites and systems.
- **We support robust technology investment** within New Zealand's critical systems by upholding the independence and rigour of our regulatory frameworks.
- **We are New Zealand's first line of cyber defence** by detecting, disrupting, analysing, and publicly identifying threats from across the cyber landscape.