NEW ZEALAND'S
Cyber Security Strategy

2015

Action Plan

newzealand.govt.nz

A LIVING ACTION PLAN WITH ANNUAL REVIEWS

New Zealand's Cyber Security Strategy provides a single cohesive framework to ensure that New Zealand is secure, resilient and prosperous online. The Strategy is accompanied by an Action Plan which sets out concrete steps to protect the country's information technology systems and ensure New Zealanders can make the most of being online.

In order to deal with a rapidly changing threat, the Action Plan will be a living document that is updated annually. Many actions are already underway – and will be on-going to maintain cyber security. The Action Plan also sets out new initiatives, some of which will need further research and consultation to test whether they are feasible, and to provide more precision about implementation. All will require on-going attention and resources.

The Action Plan has four goals. There is an introductory text for each goal, followed by four to five actions. Each action involves a number of government agencies. Many actions will involve Connect Smart, a public-private collaboration with the aim of improving cyber security.

The National Cyber Policy Office (NCPO) will produce an annual report on the Action Plan to Cabinet to evaluate progress and recommend new actions where necessary. The NCPO will also work with government agencies and Connect Smart partners to produce a public annual report on the Cyber Security Action Plan.

A secure, resilient and prosperous online New Zealand.

newzealand.govt.nz

GOAL ONE:

Cyber Resilience

NEW ZEALAND'S INFORMATION INFRASTRUCTURES CAN RESIST CYBER THREATS AND WE HAVE THE CYBER TOOLS TO PROTECT OUR NATIONAL INTERESTS

Cyber Resilience involves detection, protection and recovery from cyber incidents.

Government agencies and businesses need to have timely, actionable cyber security information and advice and be able to deal with a trusted agency when they have a cyber security incident.

It is proposed that **a national CERT[1] be established**. This institution would act as a central reporting mechanism for the full range of cyber incidents, triaging incident response to the relevant separate organisation and ensuring technical advice gets to the organisations that need it – in real-time.

A national CERT would bring together representatives and functions from a range of government agencies, non-government organisations and the private sector that currently deal with cyber incidents.

It would be an internationally recognised point of contact – an important factor given the extent to which cyber incidents are perpetrated from off-shore and the need for international cooperation to manage these incidents.

The CERT would incorporate a **threat analysis and information sharing platform**. This would improve understanding of the likelihood and impact of cyber risks facing the country.

The platform would examine existing threat patterns and techniques (i.e. the signatures or cyber "fingerprints" of malicious actors), and look out for brand new threats, including those arising from technological innovations.

Information about cyber threats can come from a variety of sources: classified intelligence, other national CERTs, the private sector, multinational ICT companies, non-government organisations and individuals.

The government should review regularly those government and private sector information infrastructure systems that are most vulnerable to threats and, if compromised, would have the most consequence for New Zealand's national interests. This ensures that New Zealand's most significant assets are protected.

Project CORTEX counters foreign-sourced, technically sophisticated or persistent cyber threats against a limited number of government and consenting private sector organisations of national significance. The detection and disruption capabilities are operated by the National Cyber Security Centre within the Government Communications Security Bureau (GCSB).

As a matter of **national security**, the government must ensure that the New Zealand Defence Force's (NZDF) networked information systems, including for command and control, logistics and operation of major platforms, are adequately protected, particularly in offshore situations. New Zealand's intelligence agencies may also use cyber tools to gather intelligence and information for the protection of New Zealand's interests.

Regular **cyber security exercises** involving public, private and international partners, are necessary to ensure preparedness for major cyber incidents. This will test the effectiveness of the national Cyber Security Emergency Response Plan, involving a detailed escalation process, and seamless coordination of technical, law enforcement, policy, communications and private sector responses.

[1] CERT was once an acronym for 'computer emergency response team'. Since 1997, CERT has been a registered trademark owned by Carnegie Mellon University and is no longer used as an acronym. New Zealand is requesting permission to use the CERT trademark.

ACTIONS	OUTCOMES	WHO?*
ACTION 1 **SET UP A NATIONAL CERT**	• Agencies, businesses and individuals have clarity about where to report cyber incidents. • Efficient triaging of cyber incidents to relevant agencies. • The impact of cyber incidents is contained – harm and reoccurrence is reduced. • There is trusted two-way sharing of information on cyber threats. • Actionable and timely advice provided to agencies, businesses and individuals • An internationally recognised contact point for dealing with cyber security incidents.	NCPO/CERT NCSC/GCSB Police DIA/GCIO NZSIS Private sector Connect Smart partners - NetSafe - NZITF
ACTION 2 **VIGOROUSLY PROTECT NEW ZEALAND'S MOST IMPORTANT INFORMATION INFRASTRUCTURES**	• The protection of New Zealand's most important information infrastructures is prioritised and reflects our evolving national interests. • Increased number of organisations receiving CORTEX malware protection services. • Increased number of instances of malware detected and disrupted. • Potential for additional support to Internet Service Providers (ISPs) is explored.	NCSC/GCSB NCPO ISPs Government agencies and private sector entities of high national interest.
ACTION 3 **USE CYBER TOOLS TO FURTHER NEW ZEALAND'S NATIONAL SECURITY INTERESTS**	• NZDF's information systems and platforms are resilient to adversary exploitation. • Threats to New Zealand's security interests are detected and averted. • Cyber tools are used in accordance with the law and subject to relevant oversight mechanisms.	NZDF GCSB MoD NZSIS
ACTION 4 **PREPARE FOR MAJOR CYBER INCIDENTS**	• Twice yearly inter-agency exercises, including the private sector and international partners. • Readiness and capability to deal with a major cyber incident, including coordinated technical, law enforcement, policy and communications responses. • Trusted relationships established with international partners.	NCPO/CERT NCSC/GCSB Police DIA/GCIO NZSIS MFAT Connect Smart partners - NetSafe - NZITF

* **DIA:** Department of Internal Affairs; **GCIO:** Government Chief Information Officer; **GCPO:** Government Chief Privacy Officer; **GCSB:** Government Communications Security Bureau; **IITP:** Institute of IT Professionals; **ISP:** Internet Service Provider; **MBIE:** Ministry of Business, Innovation and Employment; **MFAT:** Ministry of Foreign Affairs and Trade; **MoD:** Ministry of Defence; **MoE:** Ministry of Education; **MoJ:** Ministry of Justice; **NCPO:** National Cyber Policy Office; **NCSC:** National Cyber Security Centre; **NGO:** Non-Governmental Organisation **NZDF:** New Zealand Defence Force; **NZITF:** New Zealand Internet Task Force; **NZQA:** New Zealand Qualifications Authority; **NZSIS:** New Zealand Security Intelligence Service; **NZTE:** New Zealand Trade and Enterprise; **TEC:** Tertiary Education Commission.

GOAL TWO:

Cyber Capability

NEW ZEALANDERS, BUSINESSES AND GOVERNMENT AGENCIES UNDERSTAND CYBER THREATS AND HAVE THE CAPABILITY TO PROTECT THEMSELVES ONLINE

The Cyber Capability goal goes beyond promoting awareness, to focus on building cyber security capability among individuals, businesses, government agencies and organisations. Achieving this goal means that New Zealanders at all levels will have the skills and tools to protect themselves online, making it harder for malicious cyber actors to steal private data, identity information or cause damage to information systems.

Connect Smart is an on-going cyber security awareness and capability campaign. The aim is to spread the cyber security message as broadly as possible, including using Connect Smart public and private partners to build the cyber security skills of their staff, customers and supply chains. Connect Smart partners are cyber security champions working collectively to improve New Zealand's cyber security.

Small and medium enterprises (SMEs) play a huge role in New Zealand's economic growth; it is important that they are equipped to protect their business information. Targeted and accessible cyber security advice will be made available for SMEs through the Connect Smart website and activities, including an **online questionnaire** to complement the **"SME Cyber Security Toolkit"**.

A new **"cyber credentials" scheme is proposed for SMEs**. The scheme will promote to the SME audience the core actions that, if implemented properly, can make a big difference to their cyber security. SMEs can use their "cyber credentials" to demonstrate publicly to their customers and business supply chain that they have in place the key cyber security practices. The scheme will involve self-assessment and independent verification. Ultimately, if there is sufficient interest from SMEs, it could also involve a system of independent certification to ensure objective testing of cyber security practices. Carrying out these core actions provides a pathway towards more detailed cyber security standards that are already available (e.g. ISO 27000 series).

Investing in cyber security is fundamental for competitive commercial performance. A guide for **business executives** is available on the Connect Smart website to ensure cyber security is "on the agenda before it becomes the agenda".[2] Voluntary standards have been developed for **industrial control systems**, based on work led by the electricity sector.[3] These materials will be updated and expanded.

Improving and maintaining the cyber security capability of government agencies is important. The head of each government agency is responsible for the implementation of the government's **Protective Security Requirements**. These requirements include measures to protect information security such as policies relating to IT procurement, supply chain, cloud services, user access privileges, mobile devices, websites and on-line services.[4]

New Zealand's **cyber security expertise** needs to grow so that businesses and organisations can source the technical staff required to carry out ICT security. At the same time, the education and training system should produce ICT users at all levels with the skills to put in place basic cyber hygiene practices.

[2] National Cyber Security Centre, Cyber Security and Risk Management – an Executive Level Responsibility, 2013. http://www.connectsmart.govt.nz/businesses/boards-and-executive/ or http://www.ncsc.govt.nz/assets/cyber-security-risk-management-Executive.pdf

[3] National Cyber Security Standards, Voluntary Cyber Security Standards for Industrial Control Systems, March 2014. http://www.ncsc.govt.nz/newsroom/ncsc-voluntary-cyber-security-standards-for-infrastructure-operators/

[4] Protective Security Requirements, Information Security Management Protocol, December 2014. http://protectivesecurity.govt.nz/home/information-security-management-protocol/

Several **tertiary institutions** have incorporated cyber security into their ICT or computer science courses and there is a growing level of cyber security specialisation. Partnerships, including mentoring, internships, work experience and apprenticeships, between tertiary education providers and the private sector should be encouraged to ensure that courses and students are fit for purpose. The government is funding three new ICT Graduate Schools to be established in Auckland, Wellington and the South Island. These and other approaches across tertiary education may be one way for tertiary providers to work together with business to help grow cyber security capability.

More can be done at the **secondary school** level to channel students into studying ICT (which should incorporate cyber security), including appropriate qualifications, mentoring, work experience, careers and further study advice. More can also be done to integrate "cyber hygiene" and safe use of ICT into primary and secondary school lessons as a basic component of **digital literacy for all students**. By the end of 2015, 90% of schools will be connected through the Ministry of Education-funded Network for Learning (N4L) providing a safe, online learning environment for students and staff.

There is also scope to work with Connect Smart partners to support targeted cyber security courses, such as practical on-the-job training or e-learning modules for employees, or the incorporation of cyber security as a business risk for those on commerce or business management courses.

Research, largely driven by the private sector including tertiary institutions, is necessary for New Zealand to develop its own innovation capability to deal with rapidly evolving cyber risks. This includes research into adversary tactics, including test beds, modelling and malware analysis.

Such research can lead to the availability of improved defensive techniques and **commercial opportunities for New Zealand businesses** as the national and global market grows for innovative cyber security products and services.

There should be strong links between the research sector and the proposed CERT. It is also important to strengthen New Zealand cyber security research capability so that it can tap into, and leverage off, international research networks.

ACTIONS	OUTCOMES	WHO?*
ACTION 1 **EXPAND CONNECT SMART ACTIVITIES AND PARTNERSHIP**	• Media and commentators recognise Connect Smart advice as technically authoritative and trusted. • Traffic to the Connect Smart website, and social media followers, increases. • A growing range of Connect Smart partners are actively involved in promoting the Connect Smart message to their staff and clients, through their own media channels, and the Connect Smart website. • A high-level cyber security summit reinforces corporate commitment to cyber security and establishes a platform for strengthened cooperation. • There is a regular flow of public Connect Smart cyber security messages, including practical advice and tips, through multiple channels and linked to events and activities throughout the year. • Evidence through Connect Smart public surveys and research of growing cyber security awareness and capability amongst New Zealanders and businesses. • Increased number and range of Connect Smart partners.	NCPO/CERT MoE Police NCSC/GCSB DIA Private sector Connect Smart partners - NetSafe - NZITF

ACTIONS	OUTCOMES	WHO?*
ACTION 2 **IMPROVE THE CYBER SECURITY CAPABILITY OF SMALL AND MEDIUM ENTERPRISES**	• Increased website hits on the SME questionnaire shows that it has proved popular. • Positive feedback from SMEs and other businesses that the advice has been useful. • Evidence that SMEs are willing to demonstrate their "cyber credentials" through self-assessment and independent verification. • Evidence (from surveys and market research) that customers and supply chain clients prefer businesses that can demonstrate their "cyber credentials".	NCPO MBIE NZTE Connect Smart partners
ACTION 3 **BOOST THE CYBER SECURITY CAPABILITY OF THE CORPORATE SECTOR, INCLUDING NATIONAL INFRASTRUCTURE, AND THE PUBLIC SECTOR**	• Government agencies' self-assessment reports to the PSR team and Government Chief Privacy Officer demonstrate improvements in the information protection capabilities of government agencies. • Increased number of corporates, including critical national infrastructure, have implemented the "top 4" mitigations. • Critical Infrastructure, using Industrial Control Systems (ICSs) and Supervisory Control and Data Acquisitions (SCADAs), have policies and procedures in place to mitigate cyber security threats.	NZSIS DIA/GCIO/GCPO NCSC/GCSB NCPO Connect Smart partners
ACTION 4 **PROMOTE CYBER SECURITY EDUCATION AND TRAINING, INCLUDING BUILDING A CYBER SECURITY PROFESSIONAL WORKFORCE**	• Improved understanding of the extent of cyber security and/or digital literacy training at primary, secondary and tertiary levels. • Identify gaps and opportunities in the supply of cyber security training given the growing demand for a cyber security professional workforce. • A public-private taskforce stimulates new initiatives to promote effective ICT training, incorporating cyber security, and links with the private sector (e.g. scholarships, competitions, internships, work placements, workforce training).	NCPO MoE TEC NZQA MBIE DIA Connect Smart partners - NetSafe - Education institutions - IITP
ACTION 5 **SUPPORT CYBER SECURITY RESEARCH AND BUSINESS INNOVATION**	• An increase in the number of cyber security research projects funded in New Zealand. • Cyber security research projects have an impact on New Zealand's understanding and mitigation of cyber security threats. • A cyber security innovation plan stimulates New Zealand businesses, universities and research institutes to build commercial opportunities based on cyber security research, innovation and development. • A confidential survey of businesses provides an understanding of the cost and incidence of cyber insecurity to the New Zealand economy – and a benchmark is established to measure progress.	MBIE NZTE NCPO NCSC Connect Smart partners International partners

* Refer to page 4 for detail on acronyms.

GOAL THREE:

Addressing Cybercrime

NEW ZEALAND IMPROVES ITS ABILITY TO PREVENT, INVESTIGATE AND RESPOND TO CYBERCRIME

Cybercrime ranges from harmful digital communications of a criminal nature (cyberbullying), to state-sponsored theft of intellectual property. Given the broad scope of cybercrime and the range of organisations engaged, this particular goal is outlined in a separate, more detailed *National Plan to Address Cybercrime*. This Plan sets out the cybercrime problem and the challenges it poses. It outlines a range of actions to prevent cybercrime and reduce the harm to New Zealanders.

Prevention first is at the heart of the approach to cybercrime – giving New Zealanders the tools to change their online behaviour. This approach intersects closely with the Cyber Capability goal of the Strategy, particularly through investment in Connect Smart.

Lifting the government's capability to deal with cybercrime is a key priority. As new technologies emerge, new skills are required for cybercrime investigation and prosecution, including digital forensics and the ability to secure electronic evidence. Some of this is already underway as agencies work together to share tools and techniques.

It is also critical that **New Zealand's legal framework** remains fit for purpose, adapting to rapidly evolving technologies and the challenges posed by crimes across multiple jurisdictions. The Harmful Digital Communications Act 2015 is a recent development (addressing cyberbullying) and a review of the Privacy Act 1993 is underway. As the threat picture evolves, other questions will need to be considered. These may include considering giving Police the tools to address botnets; widening enforcement powers to include seeking information on care and protection matters; and the role of the Internet in funding or supporting organised criminal or terrorist groups.

Reflecting the overlapping risks across the cyber-security continuum, we need a **coordinated and accessible operational response** to cybercrime. This goal will intersect with the Cyber Resilience goal, particularly the proposal for a threat analysis tool and the establishment of a CERT.

International cooperation is essential. Most cybercrimes originate outside New Zealand's borders. Successful investigation and prosecution requires interaction between law enforcement agencies from different countries. Building trust and cooperation, and sharing best practice, between the law enforcement agencies of different jurisdictions helps to ensure that the rule of law is also effective in cyberspace. This requires continued work with key partners, such as efforts to support cyber capacity building activities in the Asia-Pacific region. A further step involves progressing New Zealand's accession to the Council of Europe Convention on Cybercrime. The Convention is the first international treaty to address cybercrime by promoting harmonised legal frameworks, improving investigative techniques and increasing cross-border cooperation.

ACTIONS	OUTCOMES	WHO?*
ACTION 1 **BUILD CAPABILITY TO ADDRESS CYBERCRIME**	• Cybercrime and electronic evidence training programmes enable frontline responders to deal appropriately with situations involving cyber elements. • New Zealand Police meet Australia New Zealand Policing Advisory Agency (ANZPAA) standards.	Police
ACTION 2 **ADAPT NEW ZEALAND'S POLICY AND LEGISLATIVE SETTINGS FOR THE DIGITAL AGE**	• Test whether agencies have appropriate and effective powers and legislative framework to respond to cybercrime. • Law enforcement can swiftly respond to and investigate threats, including those emanating from outside New Zealand.	MoJ Police NCPO DIA NZSIS
ACTION 3 **ENHANCE NEW ZEALAND'S OPERATIONAL RESPONSE TO CYBERCRIME**	• New Zealanders know where to go for help with cybercrime through one single point for reporting. • Better cybercrime reporting information is available and can inform government decision-making. • Cybercrime is clearly reflected in crime reporting in New Zealand.	Police/CERT DIA GCSB NZSIS NCPO NGOs Private Sector
ACTION 4 **USE NEW ZEALAND'S INTERNATIONAL CONNECTIONS TO FIGHT CYBERCRIME**	• Cross-border access to cybercrime information is significantly improved, including through possible accession to the Council of Europe Convention on Cybercrime (also known as the Budapest Convention). • Agencies can leverage international relationships in responding to cybercrime. • Cybercrime in the Asia-Pacific region is reduced through working with countries in the region to identify gaps in their capacity to respond to cybercrime and providing targeted assistance.	MoJ NCPO MFAT Police DIA

* Refer to page 4 for detail on acronyms.

GOAL FOUR:

International Cooperation

NEW ZEALAND PROTECTS AND ADVANCES ITS INTERESTS ON CYBERSPACE ISSUES INTERNATIONALLY

International engagement is essential for cyber security. The trans-boundary nature of cyberspace means the outcomes of international debates will affect how New Zealanders use and access the online world. International cooperation underpins the other goals of the Strategy.

New Zealand supports the maintenance of a **global Internet** which ensures that all users are able to access, create and share information regardless of their location. This openness underpins the unique value of cyberspace, allowing it to act as an enabler of social and economic development. The benefits of connectivity depend on continuation of an open, innovative and secure cyberspace and, to ensure this, we need international partnerships.

This includes developing **norms and rules of the road**, engaging in discussion about how international law applies online, and contributing to international debate on technical **Internet governance** and the evolving role states play in cyberspace. New Zealand needs to be active in these discussions to protect our interests. This involves deepening policy cooperation with a broad range of traditional and non-traditional partners, including other governments, industry and civil society. This will provide operational benefits, an opportunity to broaden support for key tenets of our vision for cyberspace and contribute to international cyber stability. New Zealand has recently become a member of the Freedom Online Coalition: a group of governments committed to working together to support Internet freedom and protect fundamental human rights online.

Sharing threat information and best practice with international partners helps New Zealand to assess the cyber threat and put in place systems to address it. **Cooperation and joint operations with international partners** are essential to mitigating threats to New Zealand. Cybercrime investigation and prosecution requires close international law enforcement cooperation and raises complex jurisdictional issues.

Improving confidence and understanding of cyber security issues is an important component of international stability. With particular **focus on the Asia-Pacific region**, New Zealand contributes to building cyber security capability in developing states, assists in the development of confidence building measures and cooperates on emergency responses to cyber incidents, including through exercises. New Zealand is one of 42 founding members of the Global Forum on Cyber Expertise (GFCE), launched at the 4th Global Conference on Cyber Space in the Hague in 2015. The GFCE is intended to give momentum to global cyber security capacity building.

Being recognised as a cyber secure country is important for New Zealand's international credibility – including the **ability of businesses to be internationally competitive** and the attractiveness of New Zealand as a place to store data. New Zealand will need to work with key trading partners to ensure any cyber security measures put in place are not an impediment to New Zealand businesses.

ACTIONS	OUTCOMES	WHO?*
ACTION 1 **PROMOTE INTERNET GOVERNANCE AND NORMS OF STATE BEHAVIOUR THAT REFLECT NEW ZEALAND'S INTERESTS**	• New Zealand advances its interest in maintaining a free, open and secure cyberspace. • New Zealand participates in international discussion on appropriate state behaviour in cyberspace and is recognised as a constructive partner. • New Zealand's cyber infrastructure is safeguarded through international engagement on technical Internet governance matters. • New Zealand contributes to international discussions about how international law applies online, including how to manage national security interests and human rights obligations in cyberspace.	MFAT NCPO MBIE MoD NZDF NZITF and other stakeholders
ACTION 2 **BUILD NETWORKS OF INTERNATIONAL OPERATIONAL COOPERATION**	• International information sharing networks enable operational agencies to draw on international expertise for the protection of New Zealand systems and preventing and/or investigating cybercrime and other threats. • International links enable agencies to access cyber training and development opportunities. • New Zealand participates in joint cyber incident response management and crisis response exercises and initiatives with security partners and Asia-Pacific partners.	NCSC Police MoJ MFAT MoD NZDF NZITF and other operational partners
ACTION 3 **CONTRIBUTE TO INTERNATIONAL CYBER SECURITY CAPABILITY AND CONFIDENCE**	• New Zealand capacity building helps to raise regional cyber capability, including through provision of assistance in the Pacific. • New Zealand helps to build consensus on cyber confidence building measures in the Asia-Pacific region, including through the ASEAN Regional Forum. • New Zealand engages with key partners (including in the Pacific) to build confidence, pursue practical cooperation and, where needed, ensure New Zealand's concerns are registered.	MFAT NCPO MBIE Police NZITF and other stakeholders
ACTION 4 **MAXIMISE THE ECONOMIC OPPORTUNITIES OF CYBERSPACE FOR NEW ZEALAND AND NEW ZEALANDERS**	• New Zealand engages with trading partners on the development of their national cyber security practices to ensure new requirements do not establish barriers to trade. • Mutual recognition/equivalence of cyber security measures with trading partners are pursued. • Engage with industry to understand, and consider how to address, any cybersecurity related impediments to trade.	MFAT NCPO MBIE NZTE Connect Smart partners

* Refer to page 4 for detail on acronyms.

newzealand.govt.nz