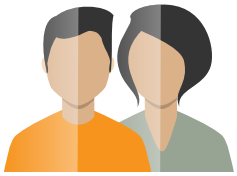


NEW ZEALAND'S
Cyber Security Strategy

2015

A secure, resilient and prosperous
online New Zealand

newzealand.govt.nz

Ministerial Foreword

The internet and technology have become a fundamental element in our lives.

We use the Internet to connect with friends and family, access government and commercial services, conduct business, store vital data, and operate national infrastructure, including telecommunications, energy and transportation systems.

New Zealand has benefited enormously from connectivity and the innovations offered by technology. Technology has accelerated our global connections and transformed almost every sector of the economy.

While connectivity has opened up significant economic opportunities, it has also led to vulnerabilities. The threat to New Zealanders, and the New Zealand economy from cyber intrusions is real and growing, and there are serious implications for our economic well-being and national security.

Perpetrators can range from a lone hacker through to organised criminal groups, activists or state-sponsored actors who operate domestically and internationally.

It's estimated that cybercrime has cost New Zealand almost $257 million in the past year.

More than 80 per cent of New Zealanders have experienced a cyber-security breach, yet only 39 per cent have changed anything about their online behaviour as a result.

56 per cent of businesses have been attacked at least once per year. Only 65% of businesses are confident that their information technology security systems are effective.

In order to make the most of the opportunities a digital economy offers, it is vital we place a strong focus on securing our information systems and building the skills across the economy to prevent cyber intrusions happening. Improving our ability to handle cybercrime and engaging with other countries on cyber security issues and the international management of the Internet is also important.

That's why we're launching a refreshed New Zealand Cyber Security Strategy and Action Plan which will provide a framework for the government to improve New Zealand's cyber security.

The Strategy emphasises that there is no simple fix and, while technological defences are effective, better cyber security will require a multi-layered approach.

As technology evolves, so too will the threats, so the Action Plan will be monitored and reviewed on an annual basis.

We'll be working across relevant government agencies and will be looking for private sector support as well. Implementing the Strategy's Action Plan will require an effective joint effort if we want to improve New Zealand's cyber security and achieve our vision of a secure, resilient and prosperous online New Zealand.

Hon Amy Adams
Minister for Communications

newzealand.govt.nz

TECHNOLOGY IS TRANSFORMING NEW ZEALAND

The Internet and other information technologies have transformed the way New Zealanders live. Connectivity is an integral part of New Zealand's economic growth and international competitiveness.

Ninety percent of New Zealand households and 96 percent of businesses now have an Internet connection. New Zealanders rely heavily on the Internet for work, play and everyday life. People are embracing the benefits the technology provides:

- Individuals are connecting to friends and family and shopping, banking, and being entertained and educated through the Internet
- Businesses are promoting their services, selling, banking and communicating using the Internet. They use information technology to manage their business information
- The government is heavily reliant on technology for the country's day-to-day administration and it is essential for the operation of our critical infrastructure

By 2019, there will be 24 billion networked devices and connections, with global Internet traffic up to 168 exabytes per month.[1]

WHAT IS CYBERSPACE?

The global network of interdependent information technology infrastructures, telecommunication networks and computer processing systems in which online communication takes place.

Cyber attacks are increasing and can cause significant damage

Increased connectivity, however, provides increased opportunities for people and groups with criminal, hostile or offensive intentions. Every year, we are detecting more cyber incidents than the year before.

- NetSafe recorded 8,061 cyber incidents in 2014, with losses through scams and fraud of almost NZ$8 million (up from 3,317 cyber incidents in 2013 with losses of more than NZ$4.4 million).
- In the 12 months to 31 December 2014 the National Cyber Security Centre recorded 147 cyber incidents. In the first six months of 2015, 132 incidents have been recorded. It is expected that by the end of 2015 this figure will be in excess of 200.
- The Department of Internal Affairs Electronic Messaging Compliance Unit received 8,786 complaints of unsolicited commercial electronic messages (email, SMS or text) in 2014-15 (up from 7,747 in the 2013-14 period).

The impacts of cyber attacks can range from a minor inconvenience through to a major system failure. At the severe end, cyber attacks have the potential to cause real harm – financial losses, reputational damage, intellectual property theft, damage to services and operations, or disruption of critical national infrastructure.

It is difficult to obtain adequate information on either the incidence or the cost of cyber incidents. Victims, including businesses, often do not report incidents to law enforcement or disclose them publicly.

[1] http://newsroom.cisco.com/press-release-content?articleId=1644203: last accessed 28/10/2015.

HOW DO NEW ZEALANDERS BEHAVE ONLINE?

Connect Smart research on New Zealander's cyber security practices (2014):

83%
of New Zealanders have experienced a cyber breach – 22% had their email accounts hacked for example.

61%
have not changed their behaviour as a result.

83%
of New Zealanders rarely change their passwords.

28%
use more complex passwords for certain sites, such as banking.

34%
of New Zealanders do not have passwords on their personal smartphones.

48%
do not have passwords on their work smartphones.

67%
of New Zealanders check a website is secure before using it for payments.

18%
of New Zealanders are overwhelmed by cyber security.

73%
want more advice.

26%
of New Zealanders believe they are not personally at risk of a cyber attack.

What does a cyber attacker look like?

Cyber risks include state-sponsored espionage, cyber vandalism or issue-motivated hacktivism, a broad range of cybercrime (e.g. scams and fraud), and deliberate or inadvertent actions by employees or contractors.

Malicious cyber actors are constantly changing their methods and tactics, often re-emerging in different guises or exploiting vulnerabilities before they are patched. They can act stealthily and anonymously online, leaving few clues, and operating from any Internet-connected location globally. This makes it hard to distinguish between the actions of state-sponsored cyber intruders, organised cyber-criminal groups or an isolated computer hacker.

New Zealand faces cyber risks because of the importance of its information assets, the inevitable weaknesses or gaps in the protection of these information assets, and the existence of attackers who can exploit these vulnerabilities for their own advantage.

A secure, resilient and prosperous online New Zealand

New Zealand faces on-going cyber risks. Malicious cyber techniques can be deployed from any location. New Zealand's geographic isolation offers no protection against cyber threats.

This Strategy sets out what government will do, working in partnership with the private sector, to prevent and respond to a range of cyber security threats. A range of actions are required.

OUR VISION IS THAT NEW ZEALAND IS SECURE, RESILIENT AND PROSPEROUS ONLINE

Achieving this vision means that individuals are protected online and New Zealand's businesses can function, grow and innovate. Cyber security has the potential to be used as a point of positive competitive advantage internationally.

Ensuring New Zealand is secure and resilient online is an essential component of building a more competitive and productive economy. This is a government priority.

New Zealand's scale and relatively simple telecommunications and network structure enables the public and private sector to work closely together to embed a cyber security culture, and to respond nimbly to evolving cyber risks.

This Strategy will mean New Zealand is a place where:

- New Zealanders and their businesses prosper;
- the harm from cyber threats and cybercrime is reduced;
- fundamental rights online are protected;
- significant national information infrastructures are defended; and
- New Zealand is respected internationally as a secure place to do business and store data.

The Strategy has four intersecting goals:

CYBER RESILIENCE

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.

This goal is about ensuring New Zealand's most significant assets are protected, that agencies may use cyber tools to further New Zealand's national security interests, and to ensure preparedness for major cyber incidents.

CYBER CAPABILITY

The Cyber Capability goal goes beyond promoting awareness to focus on building cyber security capability among individuals, businesses, government departments 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.

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. Investing in cyber security is fundamental for competitive commercial performance. New Zealand's cyber security expertise also needs to grow so that businesses and organisations can source the technical staff required to carry out ICT security.

ADDRESSING CYBERCRIME

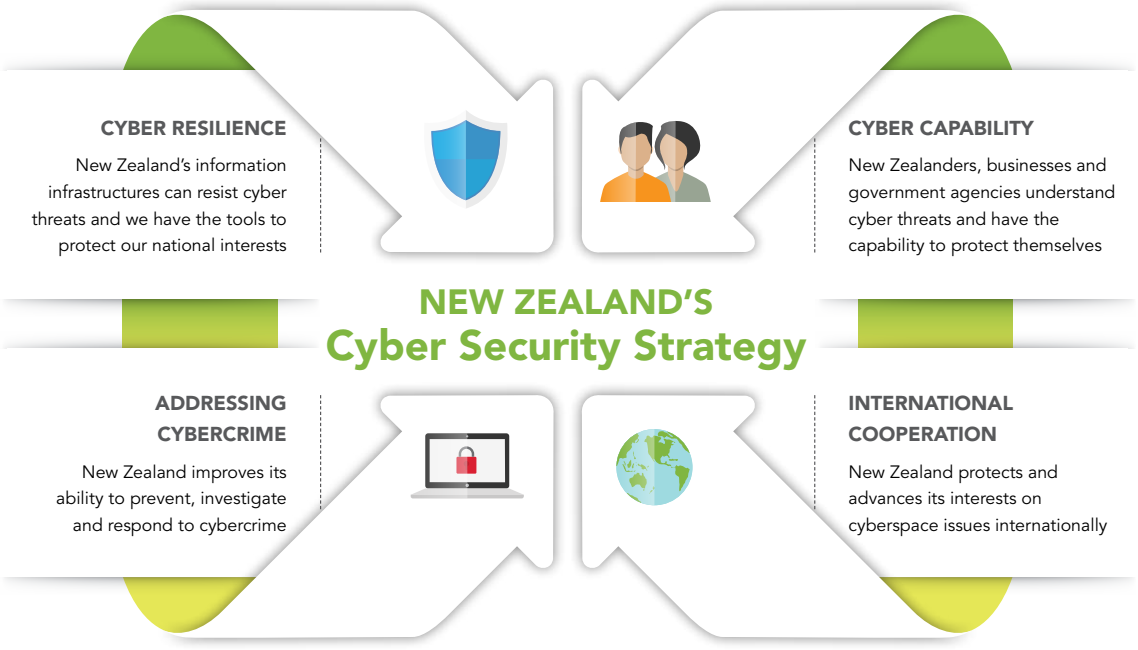
Cybercrime ranges from harmful digital communications of a criminal nature (cyberbullying), to state-sponsored theft of intellectual property. Given the broad scope of cybercrime and the range of organisations engaged, this particular goal is outlined in a separate, more detailed *National Plan to Address 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. A joined-up approach will also be critical to provide an effective, customer-focused response to cybercrime.

INTERNATIONAL COOPERATION

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.

The benefits of connectivity depend on continuation of an open, innovative and secure cyber space. To ensure this we need international partnerships, with a particular focus on the Asia-Pacific region. Being recognised as a cyber secure country is important for New Zealand's international credibility – including the ability of businesses to be internationally competitive. 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.



Delivering the vision: The Action Plan

To deliver the vision, the government has developed a plan of action to bring each of the four goals to life. The Action Plan will be reviewed and reported on annually, and changes made to keep the Strategy alive and current. The National Cyber Policy Office will also work with government agencies and Connect Smart partners to produce a public annual report on the Cyber Security Action Plan.

The Strategy is underpinned by four principles:

PARTNERSHIPS ARE ESSENTIAL

The government has a role to play in cyber security – but not on its own. Close partnerships with the private sector and non-government organisations are required. Businesses drive the New Zealand economy and depend on the Internet and networked technology. They must protect the information that is critical to their commercial success. The private sector owns and operates the telecommunications systems. The private sector and technical community also have considerable cyber security expertise.

connect SMART
Protect yourself online

The Connect Smart partnership is a public-private collaboration focused on driving cyber security improvement in New Zealand. It includes a growing network of banks, telecommunication companies, ICT companies, software companies, social media, retail organisations, education institutions, non-government organisations, community groups, sectoral bodies, business associations and government agencies.

ECONOMIC GROWTH IS ENABLED

Strong cyber security practices will result in businesses remaining productive, profitable and transparent to customers and shareholders. New Zealand will be recognised as a desirable place to do business, store data, innovate and invest.

ICT and enhanced connectivity will continue to boost economic growth, and the costs of cyber insecurity will be minimised.

NATIONAL SECURITY IS UPHELD

Cyber threats to New Zealand, particularly state-sponsored espionage, cyber terrorism, theft of intellectual property from government and critical national infrastructure, are national security risks. Upholding New Zealand's national security in the face of this threat is a fundamental principle of this Strategy.

HUMAN RIGHTS ARE PROTECTED ONLINE

The openness of the Internet is part of its unique value – allowing for unrestricted participation and the free flow of information.

Cyberspace should be a trusted medium, where users have confidence in the integrity of information and the protection of their private and financial details. They should be able to engage online without suffering harm or unlawful interference.

Human rights apply online as they do offline. This includes the right to freedom of expression, and the protection of privacy, as set out in New Zealand law and existing international law.

WHAT HAS NEW ZEALAND DONE SO FAR?

POLICE ELECTRONIC CRIME GROUP ESTD 1984

ONLINE CHILD EXPLOITATION ACROSS NZ (OCEANZ) SPECIALIST POLICE UNIT ESTD

2011 NZ CYBER SECURITY STRATEGY

NATIONAL CYBER SECURITY CENTRE ESTD WITHIN GCSB 2011

NATIONAL CYBERCRIME CENTRE ESTD OCT 2009. NOW CALLED THE POLICE CYBER CRIME UNIT

NATIONAL CYBER POLICY OFFICE ESTD, JUNE 2012

NGOs, such as NZ Internet Taskforce and Internet NZ, provide a forum for cyber security collaboration

Government's Protective Security Requirements, incl Information Security Manual launched (Dec 2014)

DIA/NZ POST ESTABLISH 'REAL ME' PROVIDING A VERIFIED ONLINE ID AND SECURE LOG-IN

PREVENTION FIRST: POLICE NATIONAL CYBERCRIME OPERATING STRATEGY

TELECOMMUNICATIONS (INTERCEPTION CAPABILITY AND SECURITY) ACT (TICSA) 2013

NETSAFE ESTD 1998 – EDUCATION AND RESPONSE SERVICES

Office of the Privacy Commissioner focus on technology and privacy with its "Making the Future" strategy (Dec 2014)

NCSC DEVELOPMENT OF VOLUNTARY STANDARDS FOR ELECTRICITY SECTOR/INDUSTRIAL CONTROL SYSTEMS 2013

DIA ELECTRONIC MESSAGING COMPLIANCE TEAM ESTD

CYBER SECURITY AWARENESS CAMPAIGNS 2012, 2013

CAPACITY BUILDING IN THE ASIA-PACIFIC REGION

International engagement on norms of State behaviour in cyberspace (e.g. London agenda)

GOVT ICT STRATEGY AND WORK TO IMPROVE SECURITY AND PRIVACY OF GOVERNMENT INFORMATION

GCSB SUPPORT TO GOVT AGENCIES AND PRIVATE SECTOR AGAINST ADVANCED THREATS (CORTEX)

GCSB ACT 2013 – INFORMATION ASSURANCE AND CYBER SECURITY A CORE FUNCTION

INTERNATIONAL ENGAGEMENT ON INTERNET GOVERNANCE (E.G. ICANN)

CYBER EMERGENCY RESPONSE PLAN AND EXERCISES 2012, 2013, 2014

ESTD 2014
connect SMART
Protect yourself online

newzealand.govt.nz