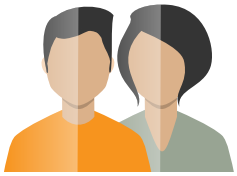


NEW ZEALAND'S
Cyber Security Strategy

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

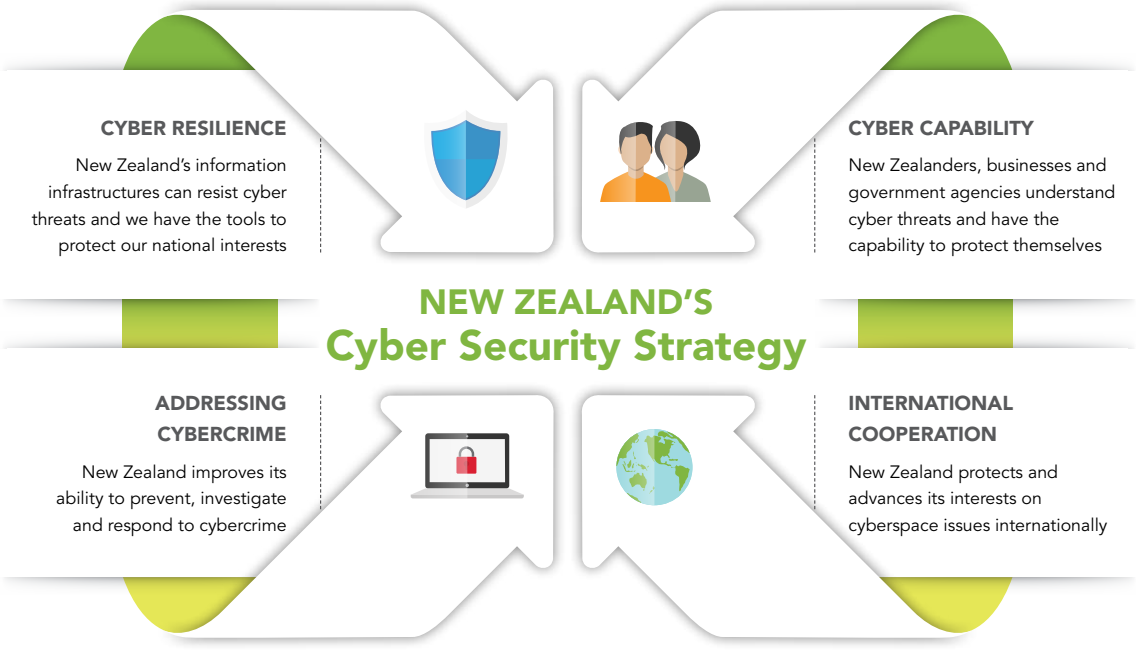
Cybercrime ranges from harmful digital communications of a criminal nature (cyberbullying), to state-sponsored theft of intellectual property. Given the broad scope of cybercrime and the range of organisations engaged, this particular goal is outlined in a separate, more detailed *National Plan to Address 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

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

National Plan to Address Cybercrime

2015

Improving our ability to prevent, investigate and respond to cybercrime

newzealand.govt.nz

Contents

A secure, resilient and prosperous online New Zealand.

newzealand.govt.nz

INTRODUCTION

New Zealanders live in a connected world. The Internet and information communications technologies (ICT) have broken down geographical barriers, brought people together and created opportunities for economic growth and innovation. New Zealanders' private and professional lives are underpinned by digital technologies as never before. Government, business, non-governmental organisations and individuals are seizing the opportunity to deliver services, transact business and communicate in cyberspace.

The cyber environment also provides opportunities for those with criminal or hostile objectives. The scale, speed and global nature of cybercrime present a challenge to traditional law enforcement methods and skills, and to confidence in our online world.

Purpose of the National Plan to Address Cybercrime

New Zealand's Cyber Security Strategy 2015 has four goals: Cyber Resilience, Cyber Capability, Addressing Cybercrime and International Cooperation. The National Plan to Address Cybercrime (the Plan) has been developed to support the cybercrime goal and contribute to the delivery of the Strategy's vision: **"A secure, resilient and prosperous online New Zealand"**.

The Plan sets out the New Zealand government's understanding of the cybercrime issue, principles and actions to improve our ability to prevent, investigate and respond to cybercrime and reduce harm to New Zealanders.

It will ensure New Zealand's response to cybercrime is coordinated at a national and international level, while also providing individuals and businesses with the tools to protect themselves.

What is cybercrime?

Cybercrime is part of a continuum of activity that ranges from cyber safety challenges to threats to national security. Cybercrime can encompass criminal activity from cyberbullying to state-sponsored theft of intellectual property. Cybercrime can be devastating to individuals, communities and business at both ends of the scale.

For the purposes of this Plan, **the definition of cybercrime has two elements.**[1]

- A criminal act that can only be committed through the use of ICT or the Internet and where the computer or network is the target of the offence. This is regardless of what the criminal goal is – whether political or financial gain, espionage or any other reason. Examples of cybercrime include producing malicious software, network intrusions, denial of service attacks and phishing.
- Cyber-enabled crime is any criminal act that could be committed without ICT or the Internet, but is assisted, facilitated or escalated in scale by the use of technology. This includes a vast amount of serious and organised crime, such as cyber-enabled fraud or the distribution of child exploitation material.

However, cybercrime is a subset of general crime, and the boundaries will not always be hard and fast.

The nature of the cybercrime problem and the challenges for New Zealand

THE COSTS OF CYBERCRIME ARE DIFFICULT TO CALCULATE RELIABLY

The extent of the cybercrime problem is not well understood. Worldwide, many instances of cybercrime go unreported. In some instances, victims will be unaware they have been affected. Other victims are too embarrassed to report the crime, do not know to whom to report, whether a crime has been committed, or do not believe law enforcement can provide a remedy. If victims receive a remedy from a supplier or financial institution, they may not also report a crime. Finally, businesses can be reluctant to disclose losses or breaches for fear of reputational damage. According to the UK Home Office, survey data suggests that in 2012, businesses reported only 2% of online crime incidents.[2] As a result, the economic cost of cybercrime is notoriously difficult to calculate reliably.[3] What we do know is that survey and anecdotal evidence indicates a high level of experience with cybercrime. One recent report estimated the annual cost to the global economy at more than US$400 billion.[4]

The indirect costs from cybercrime are equally difficult to quantify, including the opportunity costs. For many small-to-medium enterprises, cybercrime may result in 'denial of business' – nothing may be stolen, but an attack can reduce their ability to trade. Businesses and individuals also face costs to protect against cybercrime and for remediation (if required). Overseas, well-known losses include the theft of personal and financial information for 70 million customers of US retailer Target in 2013 and the theft of data related to 56 million credit cards from Home Depot in 2014. Cybercrime can also enable the organisation and perpetration of physical crime, for example fraud, extortion, disorder, sexual and other violent assaults.

[1] New Zealand Police "Prevention First: National Cybercrime Operating Strategy 2014-2017" (Wellington, 2014).

[2] M McGuire and S Dowling "Cyber crime: A review of the evidence" (Home Office Research Report 75, October 2013).

[3] Police National Intelligence Centre (NIC) "Summary from 'Cyber crime: The need to improve public confidence' (May 2014)" (New Zealand Police, Wellington, 2014).

[4] Police, 2014.

Cybercrime may result in social harms through embarrassment and nuisance and, in more serious cases, physical or emotional harm. In the Sony pictures hack in late 2014, large quantities of personal and commercial data were stolen and publicly released (in addition to triggering an international debate on freedom of expression in the digital age). Finally, while the financial losses from cybercrime can be small in an individual instance, the effects on public trust and confidence may be corrosive over time.

THERE IS NO COMPLETE PICTURE OF CYBERCRIME IN NEW ZEALAND

83%
of New Zealanders have experienced a cyber breach.

We are only seeing the tip of the iceberg. Research commissioned for Connect Smart Week 2014 found that 83% of New Zealanders had experienced a cyber-security breach.[5] This is not yet reflected in reporting, as New Zealand does not have a single, central point of reporting and breach disclosure is not mandatory. Even if they want to, victims do not always know where to report. Different agencies are responsible for different types of cybercrime, so some incidents will be reported to multiple places, while other victims may be passed from one agency to another in an effort to find the best place for a resolution.[6] Responses may also vary within each service. As a result, no one has a consolidated picture of cybercrime in New Zealand.

As the threat picture develops, we will gain a better understanding of what is required to effectively combat cybercrime, including the full ramifications of rapid technological change and emerging trends such as the rise of online or 'crypto' currencies. Related legislative reforms are already underway but further amendments are likely to be required to ensure New Zealand's legal framework is future-proof and facilitates an effective response to cybercrime.

IT IS DIFFICULT TO DETECT, INVESTIGATE AND PROSECUTE CYBERCRIME

Cybercrime produces high returns at a low cost and reasonably low risk to the criminal. Thousands of spam emails may generate small losses for each victim, but a much greater loss for New Zealand as a whole. The two most common techniques – social engineering (where a victim is tricked into granting access) and vulnerability exploitation (taking advantage of programming issues) – do not require much investment by criminals, due to the low marginal cost between one victim and thousands of victims.

Cybercrime can also be distinguished from 'traditional crimes' by the challenges its global nature presents for law enforcement. Individuals and groups overseas can operate wherever an Internet connection is present. The perpetrators are overwhelmingly based overseas and are highly organised – one United Nations report estimates that 80% of cybercrime is a part of organised criminal activity.[7] Traditional organised crime groups are migrating to this environment for greater profit at less risk.

[5] Connect Smart "Understanding Public Perceptions Toward Cyber Security" (July 2014). Last accessed 30/09/2014. http://www.connectsmart.govt.nz/assets/Uploads/Perceptive-Research-Understanding-Cyber-Security-Public-Perceptions-2014.pdf

[6] Police NIC, 2014.

[7] United Nations Office on Drugs and Crime "Comprehensive Study on Cybercrime: Draft." (February 2013). Last accessed: 24/09/14. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

The global element makes it difficult to find the perpetrator and access related evidence. Information exchange and cooperation between different countries can be poor and even where strong cooperative relationships exist, mutual legal assistance treaty processes can be very slow and cumbersome. Cases may require a disproportionate amount of investigative effort, reducing the availability of resources to deal with other demands. The country where a perpetrator is based may also not have the necessary skills or capacity to conduct a suitable investigation or preserve evidence.[8]

Investigation is further complicated by the ability to operate near-anonymously on the Internet. Attribution in cyber incidents is very difficult, particularly when an attack originates overseas. This makes cybercrime challenging not only to investigate but also to prosecute. Proxies and channels like The Onion Router (TOR) and peer-to-peer (P2P) networks can be exploited by criminals attempting to hide their identity under layers of encryption. Those networks are frequently used to facilitate criminal activity and pose challenges for law enforcement. One well-known example was the use of the now-closed 'Silk Road' site on the TOR network for drugs trading. The fastest growing is a market called 'Evolution' – advertising guns, stolen credit card data, stolen medical information and fake identification – which offers highly secure transactions.[9] Increasingly, such sites and dark markets are also selling cybercrime as a service, such as hackers for hire or simple toolkits. These developments lower the barriers for entry into cybercrime.[10]

Dark markets are selling cybercrime as a service: hackers for hire or simple toolkits.

Accordingly, a growing group of unskilled actors can have a relatively damaging impact. At the other end of the spectrum, the lines are blurring between criminal actors and state actors (some of whom may also act with criminal intent) as activity proliferates and techniques become increasingly sophisticated. As technology and detection strategies evolve, so too do the actors, making it difficult for responders to keep pace.[11] New Zealand offenders are not averse to using anonymising technology, including the use of TOR to attempt to hide sites providing child exploitation material and drug dealing.

NEW ZEALAND'S RESPONSE TO CYBERCRIME IS SHARED BETWEEN GOVERNMENT, NGOs, THE PRIVATE SECTOR AND INDIVIDUALS

A range of government agencies have policy and operational responsibilities related to cybercrime. Those roles have largely evolved organically rather than by design. At present, these include:

- **New Zealand Police:** overarching responsibility for crime prevention, detection and investigation in New Zealand, the Police Cybercrime Unit, Online Child Exploitation Across New Zealand (OCEANZ), Organised Financial Crime Agency New Zealand (OFCANZ).
- **Ministry of Business, Innovation and Employment:** Scamwatch and fraud awareness.
- **Department of Internal Affairs:** Electronic Messaging Compliance (anti-spam), Censorship Compliance Unit.

[8] Calum Jeffray and Tobias Feakin "Special Report: The Underground Web: The Cybercrime Challenge" (Australian Strategic Policy Institute, March 2015).

[9] Jeffray and Feakin, 2015.

[10] Police NIC, 2014.

[11] Police NIC, 2014.

- **Department of the Prime Minister and Cabinet:** the National Cyber Policy Office, Connect Smart.
- **Ministry of Justice:** criminal justice policy development.
- **National Cyber Security Centre** (in the Government Communications Security Bureau): advanced threats against New Zealand's information infrastructures of national importance.
- **New Zealand Customs Service:** border protection.
- **New Zealand Security Intelligence Service:** investigation of state-sponsored espionage, either directed against or involving New Zealand, with emphasis on detection and investigation of threats.
- **Serious Fraud Office:** serious or complex frauds.

However, cybercrime is a shared problem – non-governmental organisations (NGOs), civil society and the private sector all have a role to play in both prevention and response. NetSafe[12] and the New Zealand Internet Taskforce,[13] for example, provide a reporting point and incident advisories – and have taken on roles not currently provided by government. Twenty-three percent of all the reports NetSafe received in 2014 were directly referred from the New Zealand Police.[14]

The New Zealand government has also initiated Connect Smart:[15] a partnership with a range of organisations to raise awareness and capability. Many private sector companies provide a response to cybercrime as a part of their core customer service – managing cybercrime is a part of doing business in the 21st century – and build a range of protections into the services they offer.

Responsibility also sits with the wider community. The New Zealand Police's operating strategy is *Prevention First*, an approach which is also relevant to cybercrime.[16] Ideally, cybercrime will be prevented before it occurs. While there is no way to totally eliminate the risk, there are simple steps every individual can take to reduce risk. New Zealanders need to take cyber security threats seriously and be equipped with the tools and techniques to protect themselves online.

To reduce the number of cybercrime victims in New Zealand, we need to raise awareness in a way that creates behavioural change. Research commissioned as part of Connect Smart Week 2014 showed that, of the 83% of New Zealanders who had experienced a cyber-security breach, 61% had not changed their online behaviour since the breach.[17] The research also suggested that New Zealanders find the topic overwhelming, meaning there is a role for government, in partnership with the private sector and NGOs, to be a trusted source of information and advice.

Accordingly, there are opportunities for the government to improve the experience for victims of cybercrime, while also gaining a better understanding of the issue. A joined-up approach will be critical to provide an effective, customer-focused response to cybercrime. Confidence in the security and use of ICT will also be critical to achieve the government's objectives in delivering services to citizens via online channels.

[12] http://www.theorb.org.nz

[13] http://www.nzitf.org.nz

[14] Figure from NetSafe.

[15] www.connectsmart.govt.nz

[16] Police NIC, 2014.

[17] Connect Smart, 2014.

PRINCIPLES TO UNDERPIN OUR APPROACH

Four key principles underpin the New Zealand government's approach to cybercrime. Three of these are drawn from *New Zealand's Cyber Security Strategy.* The first principle (below) is specific to this Plan's cybercrime focus.

PREVENTING AND MINIMISING HARM

Initiatives and activities aimed at increasing awareness of the risks posed by cybercrime will be prioritised, with the goal of promoting behavioural change and raising capability to mitigate those risks.

ECONOMIC GROWTH IS ENABLED

Economic harm is a major consequence of cybercrime. Businesses in New Zealand – large and small – are increasingly affected by cybercrime. Ways to address cybercrime which support productivity and competitiveness will be sought.

A PARTNERSHIP APPROACH IS ESSENTIAL

The government has a role to play in cyber security – but it cannot do it alone. The cybercrime response is a shared responsibility and the New Zealand government will work in close partnership with the private sector, academia, civil society, individuals and other countries. That partnership will be based on mutual respect and trust.

The plan will seek opportunities to share experiences, best practice and to cooperate on research and development initiatives. Industry-led and targeted initiatives will be supported (for example, among the banking sector). The government will also continue to work with NGOs like NetSafe that are engaged in a range of cyber safety and security challenges on behalf of New Zealanders.

HUMAN RIGHTS ARE PROTECTED ONLINE

A key part of the New Zealand's government's approach to cyber security policy is to support the creativity, freedom, openness and dynamism that has made the Internet what it is today. New Zealanders should be able to engage online without suffering harm or unlawful interference.

PRIORITY ACTIONS

This Plan includes four priority actions. Each should be considered alongside the wider actions in the *New Zealand's Cyber Security Strategy;* all have been incorporated into the 2015 Action Plan.

1 Build capability to address cybercrime

2 Adapt New Zealand's policy and legislative settings to the digital age

3 Enhance New Zealand's operational response to cybercrime

4 Use New Zealand's international connections to combat cybercrime

PRIORITY ACTION 1

Build capability to address cybercrime

Preventing harm to New Zealanders means that increasing capability and awareness must be at the heart of any response to cybercrime, giving New Zealanders the incentives and tools to change their online behaviour. This should result in New Zealanders being alert to social engineering and other cybercrime techniques, and actively taking practical steps to protect themselves online. Law enforcement agencies will also have the capability to undertake search and evidence recovery when a crime has been committed. Success will be measured when New Zealanders know where to go for assistance and cybercrime rates reduce.

This is closely linked to the Cyber Capability goal in *New Zealand's Cyber Security Strategy.*

connect SMART
Protect yourself online

Connect Smart (www.connectsmart.govt.nz) was launched in 2014 to provide an ongoing, positive approach to cyber security, supported by a wide range of partners from across the public, private and NGO sectors.

Connect Smart is aimed at raising awareness of security and promoting ways for New Zealanders to protect themselves online.

USING THE CONNECT SMART BRAND TO PREVENT CYBERCRIME

We will continue to use the Connect Smart brand, website and partner channels to raise awareness of the cybercrime threat and promote behavioural change. Providing up-to-date alerts and information around current scams and attack vectors will help ensure New Zealanders understand the threat. Creating a clear understanding of the challenges will underpin active behavioural change by New Zealanders and foster a culture of cyber security. This will also align with initiatives like NetSafe's work with schools to 'grow digital citizens' and significant work by the Ministry of Education on digital literacy.

We will continue to provide advice, through Connect Smart, about simple tools and techniques to prevent cybercrime. It is critical that individuals and small-to-medium enterprises have up-to-date, trusted advice about what action they can take. We will work with partners to develop and distribute this advice through a range of channels, including the Connect Smart website and social media. We will also integrate Connect Smart messaging into crime-prevention initiatives and community liaison roles (such as Police community liaison officers).

DEVELOPING GOVERNMENT CYBERCRIME CAPABILITY

The *Strategy* sets out the need to develop a cyber security professional workforce and the difficulty in both attracting and retaining highly skilled people. This also applies to law enforcement. Electronic evidence is increasingly a part of many criminal investigations. New Zealand must ensure its capability keeps up with demand for these skills and emerging technologies. All front line Police officers and other investigators need, as a minimum, to be able to identify cybercrime and cyber-enabled crime. Investigators will need to be able to identify lines of enquiry and evidential material, and specialist units must have the capability to provide assistance in more complex and sophisticated cases. There must be enough skilled investigators to keep up with the rising demand for electronic evidence.

Agencies will continue to share experience, skills, knowledge and resources through the Electronic Combined Law Agency Group (e-CLAG). E-CLAG sits within the broader Combined Law Agency Group – a group of intelligence, enforcement and compliance professionals who

collaborate on a whole-of-government approach to leverage combined resources. CLAG partnerships are used to tackle the threats of cross-agency crime.

Members of e-CLAG are the digital forensic investigators and analysts from member agencies with digital forensic divisions. The field is rapidly evolving and, in some instances, an agency will only have one investigator or analyst on staff, hence a need to make use of the knowledge, experience and resources of other e-CLAG member agencies. Past and ongoing e-CLAG activities include joint agency training sessions and the provision of assistance and tools between member agencies (and to agencies without digital forensics capability). Current projects include developing a matrix capturing equipment assets and training requirements across agencies.

New Zealand Police is actively developing capability and training to deal with cybercrime. The Police *Prevention First: National Cybercrime Operating Strategy 2014-2017* sets out Police goals to develop capacity and capability to meet the growing needs around cybercrime and cyber-enabled crime. The Police Cybercrime Unit is the core Police unit that deals with cybercrime and provides Police with a central point of contact for other agencies. The Unit has recently expanded to seven staff, comprised of a mix of detectives and technical investigators.

Investments in core capability are designed to create a foundation for further development and capacity building. All front line staff (level one) will be trained to deal with customers at the front desk and triage incoming reports. Investigators (level two) will identify and follow online lines of enquiry, identify evidential material and prosecute offenders. Specialists within the Cybercrime Unit (level three) will deal with the more complex cybercrimes impacting on New Zealand businesses and our reputation. Training material will be in line with the Australia New Zealand Police Advisory Agency Training guidelines.

PRIORITY ACTION 2

Adapt New Zealand's policy and legislative settings for the digital age

Alongside increased capability, law enforcement and the national security agencies need appropriate and effective powers to investigate cybercrime. New Zealand's legislative and policy settings must adapt to new technologies and balance security and privacy. Rapid changes require a technology-neutral framework; at the same time, the global nature of cybercrime poses a challenge to traditional thinking about borders and jurisdiction. **This area of work** will be successful when New Zealand's legal framework supports a rapid and effective response to cybercrime.

LEGISLATIVE REFORM ALREADY UNDERWAY

In recognition of these challenges and other issues, legislative reform is underway in a number of related areas.

In 2014, following a report from the Law Commission, Cabinet agreed to the Ministry of Justice undertaking work to update New Zealand's privacy laws. Advances in technology since 1993 have dramatically changed how personal information is collected, stored and shared. Reform of the **Privacy Act 1993** will emphasise identifying and addressing risks before privacy breaches can occur.

The Law Commission is currently undertaking a review of the **Extradition Act 1999** and the **Mutual Assistance in Criminal Matters Act 1992**. These Acts frame New Zealand's response to requests from foreign governments in the investigation and prosecution of crime. The review is based on the effects of technological change, alongside other developments in the international context, such as globalisation, increasing mobility and transnational crime.

Law enforcement needs to operate swiftly across many jurisdictions.

The New Zealand Customs Service is in the process of reviewing the **Customs and Excise Act 1996**. The intent of the review is to ensure that the Act is flexible and permits Customs to undertake their border protection role using new technology and operating methods.

In response to rising concerns about the harmful effects of cyberbullying on young people, the **Harmful Digital Communications Act** was passed in July 2015. Under previous laws, it could be difficult for victims to deal with harmful digital communications – for example, trying to remove abusive, intimidating and distressing material from the Internet could be difficult, drawn out and costly. Also, few sanctions were available to aid such efforts and to hold offenders to account. The Act is intended to prevent harm and provide victims with quick and efficient redress. The Act has created a range of measures to address damaging electronic communications spread through methods such as emails, texts and social media posts.

DEVELOPING A BETTER UNDERSTANDING OF OUR LEGISLATIVE NEEDS

The Law Commission reviewed 'computer crime' in 1999. The drafting of legislation is technology neutral, but given technological and global developments, since then there may be a need to update or amend it.

Elements of New Zealand's legislative framework will be tested to see whether amendment to effectively prevent, investigate and respond to cybercrime is required. This would be a targeted review. Examples may include amending section 252 of the Crimes Act to permit Police to remove

botnet infections, considering widening enforcement powers to include seeking information on care and protection matters, considering whether we need an offence of unlawful possession of stolen data, reviewing the crimes involving computers provisions in the Crimes Act and the role of the Internet in funding or supporting organised criminal or terrorist groups.

Elements of New Zealand's policy and legal frameworks will be tested to see whether they need amendment to permit further preventative operational activity. Covert work currently plays an important role in investigating and preventing the online exploitation of children. Many criminal networks online rely on trust and confidence to operate so there may be opportunities to enhance a proactive approach to preventing cybercrime or responding to offenders.

MEETING TRANS-BOUNDARY CHALLENGES

Most cybercrime is perpetrated from outside New Zealand. Criminals exploit the differences between countries and evidence relating to a criminal act may sit in multiple locations.

The government will work with partners (including multinational companies) to meet the challenges raised by extraterritorial jurisdiction. Cybercrime often means that law enforcement needs to operate swiftly across many jurisdictions and to access information under many different legal and political regimes. This challenges our traditional notions of sovereignty and jurisdiction – and the issue will not be resolved by one state alone. Exploring accession to the Council of Europe Convention on Cybercrime is an important first step, as is working with companies to ensure that law enforcement and security agencies have lawful access to data.

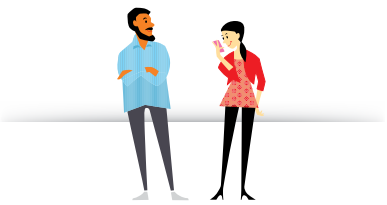
PRIORITY ACTION 3

Enhance New Zealand's operational response to cybercrime

A range of government agencies, NGOs and private sector companies play different roles in regard to cybercrime. To generate the strongest possible response to cybercrime, we need to work together and leverage our individual and collective strengths. Our measures of success will be a coordinated response to cybercrime and a better understanding of the size, nature and impact of cybercrime threats.

ENHANCING NEW ZEALAND'S RESPONSE TO CYBER INCIDENTS

As set out in *New Zealand's Cyber Security Strategy,* work is underway to establish a national CERT[18] to deal with issues across the spectrum, including cybercrime. New Zealand's cyber response capabilities have developed organically and are spread across a range of agencies. A CERT should bring some of those capabilities together and result in a more effective and efficient response for victims of cybercrime.



Making it easier for New Zealanders to report cybercrime will… help New Zealand better understand and respond to cybercrime

Ways to enhance cross-agency operational effectiveness in the prevention, investigation and response to cybercrime will be investigated. There are opportunities for agencies to share knowledge and techniques in investigations. As discussed earlier, some of this is already underway through forums like e-CLAG.

Police reporting will begin to distinguish cybercrime from other crimes. At present, it is not always possible to distinguish between crimes committed online and those committed offline. Police recording of reported incidents will need regular reviews to consider identification of cybercrime and cyber-enabled crime so that they are distinguishable from offences which are not facilitated by ICT. This will mean developing criminal behaviour is properly monitored, allowing new and developing trends to be better identified.

ENHANCING OUR CUSTOMER FOCUS

As highlighted earlier, cybercrime tends to be under-reported for a range of reasons. Making it easier for New Zealanders to report cybercrime will provide better support to victims and ensure better information is collected, to help New Zealand better understand and respond to cybercrime.

Options to establish a central point for cybercrime reporting will be considered. Options to improve customer experience will be considered by providing a single 'front door' at which issues are triaged and directed to the appropriate responder.

Victims of cybercrime have access to the same support as other victims of crime. Focusing on victims in the criminal justice system helps reduce the cost and impact of crime on individuals. Financial and emotional effects of crime on victims will be minimised and services for victims will be provided in a timely and credible way.[19]

[18] 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.

[19] www.victimsinfo.govt.nz/

PRIORITY ACTION 4

Use New Zealand's international connections to combat cybercrime

International engagement is essential for cyber security. As a result, the principle of partnership applies equally internationally as it does domestically. New Zealand is not isolated in cyberspace, which creates challenges for law enforcement in investigating and prosecuting cybercriminals. The fundamentally global nature of the problem requires a coordinated international response. This will be successful when law enforcement in New Zealand can more effectively prevent crime and respond swiftly to cybercrime threats emanating outside our jurisdiction.

CLOSER COOPERATION ON CYBERCRIME

Differences in national laws and enforcement regimes can create barriers to effective international cooperation. New Zealand is committed to working with partners to reduce those barriers. Law enforcement agencies work closely with counterparts through INTERPOL and in Australia (particularly through the Australia New Zealand Policing Advisory Agency), Canada, the United States and the United Kingdom. New Zealand is also a member of the Virtual Global Taskforce, the Global Alliance against Child Sexual Abuse Online, the ASEAN Regional Forum and the London Action Plan on spam.

Consider progressing New Zealand's accession to the Council of Europe Convention on Cybercrime (also known as the Budapest Convention). The Council of Europe Convention on Cybercrime is the first international treaty seeking to address cybercrime by promoting harmonised legal frameworks, improving investigative techniques and increasing cross-border cooperation. It was developed by the Council of Europe but a wide range of states have since acceded to the Convention, including our closest partners. As at May 2015, 45 states parties have ratified the Convention. To accede will require a National Interest Analysis to test the benefits for New Zealand, including testing the domestic policy implications.

Continue to promote governance of cyberspace and norms of state behaviour online that reflect New Zealand's vision and interests. There is not yet a clear consensus about appropriate behaviour for states in an online environment. As set out in the *Strategy's* International Cooperation goal, New Zealand will continue to participate in the development of international consensus about appropriate state of behaviour and the development of confidence-building measures, including on cybercrime.

Strengthen New Zealand's relationships with international bodies focused on addressing cybercrime. There are opportunities for New Zealand to contribute to and benefit from relationships with other law enforcement groups (such as Europol, NGOs, and specialist bodies sponsored by the private sector such as Microsoft's Digital Crimes Unit). International cooperation currently relies largely on personal and informal relationships. New Zealand must find ways to ensure these ongoing cooperative relationships are maintained and embedded. For example, New Zealand Police currently has a secondee at the INTERPOL Global Complex for Innovation – a cutting edge research and development facility, based in Singapore.

Networks of international cooperation will be built to support operational activity, through joint investigations, joint operations, intelligence sharing, growing expertise and developing models of best practice.

CAPACITY BUILDING IN THE ASIA-PACIFIC REGION

New Zealand is committed to the maintenance of stability and security in cyberspace. Improving confidence and understanding of cyber security issues is an important part of international stability. Although the national response to cybercrime is still being developed, nevertheless New Zealand is relatively well-placed to contribute to building capacity in the Asia-Pacific region. As the Pacific region becomes more connected, the opportunities for cybercriminals will increasingly affect economic growth and regional security. Pacific states are also likely to be targets for criminal activity as criminals seek legislative settings that are less likely to facilitate their arrest and conviction.

Work with Pacific island states to identify gaps in their capability to respond to cybercrime and undertake capacity building activities in the Asia-Pacific region. 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. New Zealand's capacity building activities will assist in building a more secure, open and accessible cyberspace that delivers broad-based economic and social benefits. Efforts will focus on raising awareness of the opportunities and risks cyberspace offers and ways to manage those; along with practical solutions to raise the policy and operational capacity of law enforcement and other government agencies to respond cyber security risks.

newzealand.govt.nz