NEW ZEALAND'S
Cyber Security Strategy

2016

Action Plan Annual Report

newzealand.govt.nz

Ministerial Foreword

It is my pleasure to release the first Annual Report on the implementation of the 2015 Cyber Security Strategy and Action Plan.

The Strategy provides a framework for the public and private sector to improve New Zealand's cyber security. This report outlines progress in a number of areas of the Cyber Security Action Plan – it has been a busy year.

An exciting initiative in the December 2015 Strategy was the Government's commitment to go ahead with the establishment of a national CERT.

I am pleased to report that CERT NZ will be up and running in the first half of 2017. It will become a focal point for New Zealand's response to cyber security threats.

CERT NZ will provide a central place for New Zealand individuals, businesses and government agencies to report cyber security incidents. It will then ensure that the incident is dealt with by the most relevant organisation.

CERT NZ will also be a source of trusted and authoritative advice on preventing threats and mitigating cyber security incidents.

I expect that the establishment of CERT NZ will help us build a more comprehensive picture of the size and nature of the cyber security threat to New Zealand.

CERT NZ will be the international point of contact for cyber security matters, working closely with CERTs in other countries to prevent and respond to cyber security incidents.

One of the principles underpinning the Strategy is that partnerships are essential. It is significant that many of the achievements this year demonstrate public and private sector collaboration.

For example, under the Cyber Capability goal, a Cyber Security Skills Taskforce has been set up to focus on closing the cyber skills gap. The Taskforce is comprised of cyber security experts, academics and industry representatives who are working extensively with industry to progress different pathways for people to enter cyber security professions.

In addition, work is underway on the design of a cyber credentials scheme to assist small businesses to improve their cyber security.

The Government Communication Security Bureau (GCSB) plays an important role in our national cyber resilience. The GCSB is rolling out malware detection and disruption services to a select group of public and private sector organisations of national importance.

There is also a cross-government programme to improve the capability of agencies to protect the security and privacy of their information.

New Zealand's first Cyber Security Summit was held in May 2016 to promote cyber security at the executive and governance level. Cyber security is not just a technical issue – it is a business risk that must be managed.

We are involved in regular cyber security dialogues and operational links with a range of countries to improve New Zealand's understanding of threats and the ability to coordinate a response.

I believe that good progress has been made to implement the Strategy – but there is more to be done to ensure New Zealand is secure, resilient and prosperous online.

Throughout 2017, the Government will consolidate progress in the areas mentioned above.

In addition, the Government will consider the requirements for accession to the Budapest Convention on cybercrime.

Our processes for dealing with a major cyber security incident will be further tested.

New initiatives include examining the security issues related to the Internet of Things and emerging technologies.

The Government will also focus on growing New Zealand's reputation for cyber security innovation and industry. We will look at how New Zealand can harness secure and trusted technology for competitive advantage globally.

I believe there is scope for New Zealand to use its size to respond nimbly to the cyber security threat.

I look forward to reporting on further progress in a year's time.

Hon Simon Bridges
Minister for Communications

Introduction

New Zealand is increasingly reliant on information communication technology and an open, trusted Internet. Internet connectivity is integral to New Zealand's economic growth and international competitiveness.

But this technology provides opportunities for those with criminal or hostile intentions. The 2015 Cyber Security Strategy signals the Government's commitment to ensuring New Zealand is safe, resilient and prosperous online.

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.

In December 2015, the New Zealand Government launched a refreshed Cyber Security Strategy, Action Plan and National Plan to Address Cybercrime.

This is the first Annual Report on implementation of the Strategy's Action Plan.

New Zealand's Cyber Security Strategy has four intersecting goals:

The Strategy is underpinned by four principles:

- Partnerships are essential
- Economic growth is enabled
- National security is upheld
- Human rights are protected online

The full New Zealand Cyber Security Strategy, Action Plan and National Plan to Address Cybercrime can be found at: https://www.connectsmart.govt.nz/about/governments-cyber-security-strategy/

GOAL ONE:

Cyber Resilience:

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

ACTION 1:

Set up a national CERT (Computer Emergency Response Team).

OUTCOMES	PROGRESS TO DECEMBER 2016
• 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 reduced. • There is trusted two-way sharing of information on cyber threats. • Actionable and timely advice is provided to agencies, businesses and individuals. • The CERT NZ is an internationally recognised contact point for dealing with cyber security incidents.	• Government funding of $22.2 million over four years has been secured to set up a national CERT[1]. • Cabinet agreed the functions of CERT NZ: 1. Incident response and triage 2. Situational awareness and information sharing 3. Advice and outreach 4. International collaboration and point of contact 5. Coordination of serious cyber incidents. • CERT NZ will be established, in the interim, within the Ministry of Business, Innovation and Employment (MBIE). • A project team has been set up to establish CERT NZ. The CERT NZ Director has been appointed. • The CERT NZ Establishment Advisory Board was formed in August 2016. The Board is comprised of nine members from the private sector.

[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 has received permission to use the term "CERT".

NEXT STEPS

- CERT NZ service design and stakeholder engagement.
- CERT NZ established first half of 2017.
- Consideration of future organisational form for CERT NZ.

ACTION 2:

Vigorously protect New Zealand's most important information infrastructures.

OUTCOMES	PROGRESS TO DECEMBER 2016
• The protection of New Zealand's most important information infrastructures is prioritised and reflects our evolving national interests.	• A review of the classified list of organisations of national importance is underway to ensure it remains an accurate reflection of those entities that are the most attractive to threat actors and, if compromised, would have the most consequences for New Zealand's national interests.
• Increased number of organisations receiving CORTEX malware protection services from GCSB's National Cyber Security Centre (NCSC). • Increased number of instances of malware detected and disrupted.	• GCSB's delivery of the CORTEX capabilities continues to track to plan. There is positive engagement with CORTEX customers and the number of organisations agreeing to receive CORTEX services is tracking to the overall plan. • An independent quality assurance review of the CORTEX project has concluded: "CORTEX is on track to realise the benefits set out in the project's business case". o The review noted[2]: ▪ CORTEX is well-run, achieving maturity scores not normally seen for government projects. ▪ Particular strengths exist around project leadership and management, the operation of the project board (which "discharges governance and challenge roles well") and clarity of purpose. o The project's focus is now turning to transitioning the newly-built capabilities to "business-as-usual" ownership. o More information can be found here: https://www.gcsb.govt.nz/our-work/information-assurance/#cortex
• Potential for additional support to Internet Service Providers (ISPs) is explored.	• GCSB has commenced a pilot to test a Malware Free Networks initiative. Internet Service Provider (ISP) Vodafone NZ was selected to partner with GCSB for this pilot through a competitive tender process. The pilot involves GCSB sharing cyber threat information and technology with Vodafone NZ to help Vodafone mitigate

[2] http://www.treasury.govt.nz/statesector/investmentmanagement/publications/majorprojects/pdfs/mppr-jul16.pdf

malware for a small subset of its commercial customers.

- More information can be found here: https://www.gcsb.govt.nz/our-work/information-assurance/malware-free-networks-pilot/

NEXT STEPS

- Complete the full deployment of CORTEX capabilities to NCSC customers.

ACTION 3:

Use cyber tools to further New Zealand's national security interests.

OUTCOMES	PROGRESS TO DECEMBER 2016
• NZDF's information systems and platforms are resilient to adversary exploitation.	• The New Zealand Defence White Paper launched on 8 June 2016 acknowledged that an increasing reliance on technology and information networks is creating new vulnerabilities. Important military and civilian communications, logistics, critical infrastructure and navigation systems are reliant on networked technologies such as the Internet, industrial control systems and global positioning satellites. • In the face of an increasing cyberspace threat, the NZDF will continue to develop cyber support capability to improve protection for Defence Force networks and provide dedicated support for deployed operations. • NZDF personnel participated in Exercise Cyber Flag 16 in the US in June 2016, alongside teams from the UK, US, Australia and Canada. The exercise involved the teams defending their networks and maintaining military operations in the face of simulated cyber attacks.
• Threats to New Zealand's security interests are detected and averted.	• Ongoing New Zealand Intelligence Community cyber investigations in support of New Zealand's security.
• Cyber tools are used in accordance with the law and subject to relevant oversight mechanisms.	• The Intelligence and Security Bill is currently before parliament. It is the Government's response to the First Independent Review of Intelligence and Security in New Zealand, which recommended the creation of a single, integrated and comprehensive act for the GCSB and NZSIS, and their oversight.

NEXT STEPS

- NZDF is developing the appropriate organisational and personnel arrangements to support the continued development of its cyber support capability.

ACTION 4:

Prepare for major cyber incidents.

OUTCOMES	PROGRESS TO DECEMBER 2016
• Twice yearly inter-agency exercises, including with the private sector and international partners.	• New Zealand held a cyber exercise in September 2016 relating to a simulated cyber incident affecting the New Zealand banking sector. Outcomes of the exercise have been incorporated into the review of the Cyber Security Emergency Response Plan.
• Readiness and capability to deal with a major cyber incident, including coordinated technical, law enforcement, policy and communications responses.	• The Cyber Security Emergency Response Plan was refreshed in August 2016. A more significant review of the Plan is underway and is due to be completed before CERT NZ becomes operational in the first half of 2017.
• Trusted relationships established with international partners.	• The Australian and New Zealand Prime Ministers agreed in February 2016 that Australia and New Zealand should undertake joint cyber exercises to ensure we can respond to a significant cyber incident affecting both nations, with the first joint exercise held in December 2016.

NEXT STEPS

- A further trans-Tasman cyber exercise is expected to form a component of the Australia – New Zealand cyber dialogue in the second half of 2017.
- The cyber exercise programme is working towards a major exercise in December 2017 as part of the National Exercise Programme within the national security system.

GOAL TWO:

Cyber Capability:

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

ACTION 1:

Expand Connect Smart activities and partnership.

OUTCOMES	PROGRESS TO DECEMBER 2016

• Media and commentators recognise Connect Smart advice as technically authoritative and trusted.	• Connect Smart Week 2016 achieved significant reach via traditional and social media:
	  ○ Media coverage was all positive or neutral.
	  ○ Most articles included key messages and advice about cyber security.
	  ○ The total reach of media coverage, the total cumulative audience for all publications during Connect Smart week, was an audience of 1,929,528. The Equivalent Advertising Value (EAV) of this media coverage was NZ$236,092.
	  ○ Media coverage included New Zealand Herald, the National Business Review, and Stuff.co.nz.
	  ○ There were 57,700 Twitter impressions relating to Connect Smart content from the @ConnectSmartNZ Twitter account.
	  ○ 100,983 views of Connect Smart videos on Facebook.
	  ○ 29 businesses and organisations used the #ConnectSmartWeek hashtag during Connect Smart Week.

• A growing range of Connect Smart partners are actively involved in promoting the Connect Smart message to their staff and clients, through their own channels, and the Connect Smart website.	• There are currently 150 Connect Smart partners. • During Connect Smart Week 2016 a range of partners contributed to the development of resources and actively distributed Connect Smart resources through their own channels: ○ Resources were provided to more than 600 agencies and businesses.

	○ There were 33,000 views of the NZ Police cyber security videos on Facebook. ○ There were 251,132 views of Facebook produced videos of New Zealand Ministers delivering cyber security tips, including the Prime Minister and Minister for Communications. This was posted on the Facebook NZ and Facebook Security NZ pages. ○ Connect Smart partners hosted and participated in workshops on the New Zealand Cyber Security Strategy in Auckland, Wellington and Christchurch. • Connect Smart Week 2016 resources can be found here: https://www.connectsmart.govt.nz/events/connect-smart-week-2016/
• High-level cyber security summit reinforces corporate commitment to cyber security and establishes a platform for strengthened cooperation.	• Almost 300 chief executives, board chairs and senior business leaders attended the inaugural Cyber Security Summit at the Sky City in Auckland on 5 May 2016. The Prime Minister and the Minister for Communications addressed the Summit. • A total of 24 organisations provided presenters and facilitators for discussions during the Summit. These included international presenters (Centre for Strategic and International Studies, Microsoft, FireEye, Hewlett Packard Enterprise and Google). • Media targeted included TV, radio, print and digital, with both mainstream and specialist media. The results were encouraging – total reach of the media coverage was 5.4m people and the Equivalent Advertising Value (EAV) was $1,006,153. The vast majority of coverage was positive (60%) or neutral (37%). The #cybernz16 hashtag was widely used, and trended at number one on New Zealand Twitter for the majority of 5 May throughout the Summit. • The Summit secured sponsorship from nine sponsors (Microsoft, Check Point, Google, Facebook, Deloitte, Dimension Data, KPMG, Spark and MinterEllisonRuddWatts). EY and PwC provided in-kind support. • The Summit demonstrated public-private sector collaboration in practice. Senior level attendees participated actively throughout the day, with private and NGO sector leaders leading panel discussions. This collaboration was most evident in the workshop participation with large numbers of senior managers "rolling up their sleeves" to work together on practical ways to advance New Zealand's cyber security.

	• More information about the New Zealand Cyber Security Summit 2016 can be found here: https://www.connectsmart.govt.nz/events/summit-2016/
• 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.	• Monthly newsletters are sent to all Connect Smart partners. • Connect Smart resources and articles are available on the Connect Smart website: https://www.connectsmart.govt.nz/resources/ and https://www.connectsmart.govt.nz/alertsnews/ • The National Cyber Policy Office (NCPO) promotes the Connect Smart message through regular speaking events using the Connect Smart brand.

• Evidence through Connect Smart public surveys and research of growing cyber security awareness and capability amongst New Zealanders and businesses.	• A survey commissioned by Connect Smart, following Connect Smart Week 2016, revealed that[3]:
	  ○ More people changed a password (70% v 63% pre-campaign).
	  ○ More people sought advice (70% v 63% pre-campaign).
	  ○ 8% of New Zealanders (378,887 people) took action as a result of seeing or hearing Connect Smart communications or resources.
	  ○ 13% of New Zealanders (615,691 people) report having seen or heard Connect Smart communications or resources.
	  ○ More people sought advice or training from their employer (22% v 17% pre-campaign).

• Increased number and range of Connect Smart partners.	• There is an ongoing programme of Connect Smart partner acquisition and engagement. • The Connect Smart partnership was launched in June 2014. In July 2014, there were 75 Connect Smart partners. As at February 2017, there are 150 Connect Smart partners and continuing interest in membership. • The partnership includes 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.

[3] Based on Colmar Brunton research and Statistics NZ population of 4,736,089 as at 28 Nov 2016. https://www.connectsmart.govt.nz/resources/research/

- Traffic to the Connect Smart website, and social media followers, increases.

- In the 12 months to March 2017 (including Connect Smart Week in October 2016) there have been:
    - 33,862 visits to the Connect Smart website with a total of 25,915 unique users
    - 75.98% website visitors were new users
    - Approximately 154,280 Twitter impressions, with 600+ followers
    - 988 views of YouTube Connect Smart cyber security videos.

NEXT STEPS

- Continue to provide range of cyber security resources for business and Connect Smart partners.
- Align Connect Smart with the CERT NZ advice and outreach functions.
- Connect Smart Week 2017.

ACTION 2:

Improve the cyber security capability of small and medium enterprises.

OUTCOMES	PROGRESS TO DECEMBER 2016
• 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".	• The Connect Smart online resources "How secure is your business" questionnaire and the "Connect Smart for Business: SME toolkit" provide practical advice for small businesses. The questionnaire and toolkit can be found here: https://www.connectsmart.govt.nz/businesses/ • Connect Smart resources are also available to help promote cyber security in the workplace – such as running a cyber security campaign, advice on phishing and ransomware. Tip sheets can be found here: https://www.connectsmart.govt.nz/resources/ • With the support of MBIE/Westpac Innovation as a Service (IaaS) funding, and using a business Accelerator process, an NCPO led design team has developed a cyber credential prototype. The prototype is a "Do It For Me" package of assessment, support and certification for small businesses that can be taken to scale through an online platform. The package has been tested with a sample of small businesses. Work is underway on the next steps to develop a scaled-up product for the New Zealand small business market.

NEXT STEPS

- Finalise the design of a scaled-up cyber credentials package for the New Zealand small business market.

ACTION 3:

Boost the cyber security capability of the corporate sector, including national infrastructure, and the public sector.

OUTCOMES	PROGRESS TO DECEMBER 2016
• Government agencies self-assessment reports to the Protective Security Requirements (PSR) team and Government Chief Privacy Officer (GCPO) demonstrate improvements in the information protection capabilities of government agencies.	• The first annual report on system-wide capability and maturity in privacy and protective security of government agencies was provided to the Minister of State Services at the end of June 2016. Based on self-assessments by 36 agencies (and 59 agencies in relation to privacy), the report sets the new baseline for protective security and privacy maturity across government. It found that: ○ Government agencies have undertaken realistic assessments of current protective security and privacy maturity, and have clear aspirations for improvement with associated programmes or work. ○ Ongoing focus on protective security and privacy is needed to continue to build resilient agencies. • From a system-wide perspective, the Government Chief Information Officer reports that information security remains in the top five ICT operational risks across government agencies. • From July 2015, the scope for the Government Chief Information Officer's ICT System Assurance expanded from public service, non-public service departments and seven crown agencies to include twenty District Health Boards. Annual ICT Operations Assurance Plans to the Government Chief Information Officer outline assurance over controls and other mitigations to manage ICT risks. • The SEEmail system, which secures email traffic over the Internet between participating government agencies, has been upgraded to version 3.1.
• Increased number of corporates, including critical national infrastructure, have implemented the "top 4" mitigations.	• The GCSB's National Cyber Security Centre (NCSC) engages with government agencies regularly to share best practice, advice on implementation of the New Zealand Information Security Manual, and information on the threat environment, including through its leadership of the Government Security Information Exchange. • The NCSC has led a number of Security Information Exchanges (SIE's) throughout the past year – to facilitate an increased awareness of cyber security awareness amongst critical national infrastructure, create trust-

	based sector sharing, and support the maturation of cyber security posture amongst members. • The NCSC has undertaken a number of senior executive and board-level briefings – resulting in greater awareness amongst the corporate sector. • Further, the NCSC has now commenced outreach and engagement to a wider, more diverse set of critical national infrastructure organisations (beyond its core CORTEX constituency). The aim is to raise organisations awareness and to support them to improve their cyber security resilience.
• 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.	• The NCSC provides assistance to companies to ensure the security of their ICS or SCADA systems. Primary interaction is through NCSC's leadership of the Control Systems SIE, providing for the sharing of best practice and information on the threat environment.

NEXT STEPS

- Under the Protective Security Requirements (PSR)/Government Chief Privacy Officer (GCPO) reporting process, government agency chief executives and board chairs have defined their short term (12 month) and long term (three to five year) targets for capability in privacy and protective security. Agencies are actively working to meet these targets.

- It is anticipated that PSR/GCPO reporting will continue while agencies work towards these targets. The second round of self-assessments from agencies is due in March 2017. The PSR and GCPO continue to support agencies to implement their work programmes to improve information security and privacy.

- The Government Chief Information Officer continues to work with agencies to iterate and mature their Assurance Plans over ICT Operations and embed their reporting and management activities to ensure key ICT risks are visible to Senior Management.

ACTION 4:

Promote cyber security education and training, including building a cyber security professional workforce.

OUTCOMES	PROGRESS TO DECEMBER 2016
• 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).	• A Cyber Security Skills Taskforce (the Taskforce) has been established to address the cyber security skills shortage in New Zealand. The Taskforce membership is made up of industry, academic and education representatives and is focusing on the following actions: ○ Developing a level 6 Diploma in Cyber Security, listed on the New Zealand Qualifications Framework (NZQF). ○ Working with industry to develop an internship programme for the second year of the Diploma course. ○ Developing a secondary school programme to position students for the Diploma. • Work is underway to develop the NZQF listed level 6 Cyber security qualification, with agreement from the New Zealand Qualifications Authority to proceed to consultation on the qualification demand and level. • The Taskforce is working with the Digital Skills Forum to identify and adopt a cyber security skills framework to augment a common digital skills framework.

NEXT STEPS

- Complete process for listing level 6 cyber security qualification on the NZQF, including:
    - Consultation with industry and training providers
    - Develop qualification outcome
    - Develop programme of study.
- It is expected the qualification will be developed for Semester 2, 2017.
- Report back to the Minister for Communications on other actions to build cyber security skills by end March 2017.

ACTION 5:

Support cyber security research and business innovation.

OUTCOMES	PROGRESS TO DECEMBER 2016
• An increase in the number of cyber security research projects funded in New Zealand.	• STRATUS (Security Technologies Returning Accountability, Trust and User-Centric Services in the cloud), led by the University of Waikato, is a six-year, $12.2 million cyber security project, funded by MBIE. STRATUS will create a suite of novel security tools, techniques and capabilities, which return control of data to cloud computing users. The aim is to empower users to be able to control the security of their data in the cloud and to give companies tools and services to sell. The project is now in its second year. Both University of Waikato and University of Auckland researchers received Best Paper Awards for their work on "privacy-preserving cloud-based mobile electronic voting" and "searchable encrypted databases" in international computer science conferences. STRATUS will also be channelling its research outputs into the development of related ISO standards from April 2017.
• 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.	• The United States-New Zealand Science and Technology Dialogue includes an item on "Digital Forensics for Law Enforcement Investigations".
• 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.	• There has been some analysis of data from the biennial Statistics NZ Business Operations Survey, which includes questions on ICT and security. There may be scope to adjust and update the questions in future surveys to improve understanding of businesses experience of cyber incidents and implementation of mitigating actions.

NEXT STEPS

- Promote the availability of contestable science and innovation funds, such as the NZ Investment Attraction Strategy, Callaghan Innovation grants, and MBIE's Endeavour Fund, which could be used to support cyber security research.
- Develop a cyber security innovation plan.
- Conduct further work towards establishing a benchmark of cyber security maturity for New Zealand businesses. This would include understanding business perception of cyber risks, the measures they are putting in place to manage this risk, business experiences of breaches and, if breaches have occurred, the impact, steps taken to deal with the breach, and the outcomes.

GOAL THREE:

Addressing Cybercrime:

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

ACTION 1:

Build capability to address cybercrime.

OUTCOMES	PROGRESS TO DECEMBER 2016
• Cybercrime and electronic evidence training programmes to enable frontline responders to deal appropriately with situations involving cyber elements. • NZ Police meet Australia New Zealand Policing Advisory Agency (ANZPAA) guidelines.	• NZ Police have developed the content of the Level One and Level Two cyber training. • Two pilot courses of the Level Two training have been run.

NEXT STEPS

- Roll out of Level One and Level Two training will commence once funding is approved.
- The need for what was originally envisaged as Level Three (specialist training) will be reviewed following finalisation of Level One and Level Two training. Aspects of what was originally planned to be Level Three Training are likely to be incorporated within Level Two.

ACTION 2:

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

OUTCOMES	PROGRESS TO DECEMBER 2016
• 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.	• Work will be led by Ministry of Justice but, due to other priorities, has not yet begun. • The Law Foundation has launched the $2 million research fund, "Information Law and Policy Project," aimed at helping New Zealand to prepare for the challenges of the information age. • Funding for the approved agency under the Harmful Digital Communications Act was approved in Budget 2016. NetSafe was appointed as the "approved agency" effective from 1 November 2016 when the Act came into force. The Act provides for a civil enforcement regime, enabling victims to seek redress for harmful digital communications (for example, removing material from the Internet with the assistance of NetSafe or through the District Court if needed). • The Ministry of Justice and the Law Commission have published an issues paper on a joint review of the Search and Surveillance Act 2012 and are due to report to the Minister of Justice by the end of June 2017. The review is considering whether law enforcement agencies should be able to require service providers to preserve specified computer data temporarily while a warrant or order to access that data is sought.

NEXT STEPS

- Further work to test New Zealand's legislative settings for the digital age.

ACTION 3:

Enhance New Zealand's operational response to cybercrime.

OUTCOMES	PROGRESS TO DECEMBER 2016
• New Zealanders know where to go for help with cybercrime (there is a 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.	• See Goal One, Action 1 on establishing a national CERT.

NEXT STEPS

- Refer to Goal One, Action 1 on establishing a national CERT.

ACTION 4:

Use New Zealand's international connections to fight cybercrime.

OUTCOMES	PROGRESS TO DECEMBER 2016
• Cross-border access to cybercrime information is significantly improved, including through possible accession to the Council of Europe Convention on Cybercrime (known as the Budapest Convention).	• The Council of Europe's Convention on Cybercrime (known as the Budapest Convention) requires States to adopt measures enabling law enforcement agencies to order preservation of computer data for up to 90 days. This is one of the main barriers to New Zealand acceding to the Convention. • The Ministry of Justice and the Law Commission have published an issues paper on a joint review of the Search and Surveillance Act 2012 and are due to report to the Minister of Justice by the end of June 2017. The review is considering whether law enforcement agencies should be able to require service providers to preserve specified computer data temporarily while a warrant or order to access that data is sought. The outcomes of this process may be relevant to considering accession to the Budapest Convention.
• Agencies can leverage international relationships in responding to cybercrime.	• NZ Police have strong international relationships with counterpart law enforcement agencies and other international bodies. This includes building relationships with major private sector organisations, such as application service providers. • NZ Police no longer have a presence in the Interpol Complex for Global Innovation in Singapore due to resource constraints. • Depending on funding, decisions will be taken on the possibility of participation in other key international cybercrime units such as European Cybercrime Centre within Europol and International Cybercrime Coordination Cell within the FBI.
• 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.	• NZ Police supported the Commonwealth Pacific Regional Cyber Crime Criminal Justice Training workshop in Tonga, March 2016. The workshop involved ten Pacific Island countries and discussed common challenges inhibiting detection, investigations and prosecutions of cybercrime and related crime in the region. • NZ Police also provide support to Pacific Island countries on specific investigations and operations.

NEXT STEPS

- NZ Police is considering the possibility of participation in other key international cybercrime units such as European Cybercrime Centre within Europol and International Cybercrime Coordination Cell within the FBI.

GOAL FOUR:

International Cooperation:

NEW ZEALAND PROTECTS AND ADVANCES ITS INTERESTS ON CYBERSPACE ISSUES INTERNATIONALLY.

ACTION 1:

Promote Internet governance and norms of state behaviour that reflect New Zealand's interests.

OUTCOMES	PROGRESS TO DECEMBER 2016
• 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 contributes to developing norms of state behaviour online, including through regular Five Eyes cyber groups, the inaugural cyber dialogue with China (Wellington, February 2016), ASEAN Regional Forum workshops, in other forums including Singapore International Cyber Week, and through active participation in relevant UN fora.
• New Zealand's cyber infrastructure is safeguarded through international engagement on technical Internet governance matters.	• New Zealand government agencies (MFAT and MBIE) participated in the UN General Assembly high level meeting to review the implementation of the outcomes of the World Summit on the Information Society, and the associated preparatory meetings in New York in late 2015.
• 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.	• New Zealand has engaged with the Internet Corporation for Assigned Names and Numbers (ICANN), including on the completed transition of IANA (Internet Assigned Numbers Authority), with the objective of maintaining a stable and secure global Internet. The transition occurred on 1 October 2016, and means that oversight over IANA will now be performed by the ICANN multi-stakeholder community rather than the United States government. • New Zealand participated in the Tallinn Manual 2.0 consultations, in The Hague in February 2016, focusing on the application of international law online. The final Tallinn Manual 2.0 was released in February 2017.

NEXT STEPS

- Internet governance and norms of state behaviour online will feature in both established and new cyber dialogues with priority cyber partner countries (see Action 2 below).

- Participation in the Global Cyberspace Conference, the primary multilateral/multi-stakeholder forum on these issues, scheduled for late 2017 in India.

ACTION 2:

Build networks of international operational cooperation.

OUTCOMES	PROGRESS TO DECEMBER 2016
• 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.	• Participation in Five Eyes cyber groups provides useful opportunities to share information and best practice – this has been particularly useful in developing the business case for CERT NZ. • The New Zealand Minister for Communications and the Australian Minister Assisting the Prime Minister for Cyber Security discussed cyber security issues in October 2016. The Australia – New Zealand Cyber Security Dialogue in December 2016 agreed on a range of initiatives for bilateral cooperation. This included trans-Tasman cooperation on cyber credentials, cyber skills, capacity building in the Pacific Island countries, CERT-CERT links, exercises, awareness raising campaigns, and cyber security challenges. These initiatives have also been reflected in Australia – New Zealand Prime Ministers' Joint Statements (February 2016 and 2017). • The National Cyber Security Centre participates in a number of international cyber security forums, many involving foreign cryptologic partners and IT security professionals. • New Zealand hosted the International Watch and Warning Network (IWWN) in June 2016 – an organisation of 15 countries (CERTs) focussed on sharing information to build global cyber situational awareness and incident response capabilities. There are monthly virtual IWWN meetings to support ongoing multilateral cooperation and access to information sharing platforms. CERT NZ intends to lead this relationship from mid-2017. • New Zealand attended the Forum of Incident Response and Security Teams (FIRST) in Seoul, June 2016. FIRST brings together a variety of security and incident response teams from the government, commercial, and academic sectors. • NZ Police supported the Commonwealth Pacific Regional Cyber Crime Criminal Justice Training workshop in Tonga, March 2016. The workshop involved 10 Pacific Island countries and discussed common challenges inhibiting detection, investigations and prosecutions of cybercrime and related crime in the region. • NZDF personnel participated in Exercise Cyber Flag 16 in the US in June 2016, alongside teams from the UK, US,

Australia and Canada. The exercise involved the teams defending their networks and maintaining military operations in the face of simulated cyber-attacks.

- NCPO and MFAT participated in ASEAN Regional Forum cyber security workshops, which included table top exercises simulating responses to a cyber incident.

- New Zealand and India agreed to cooperation and dialogue on cyber issues during the New Zealand Prime Minister's visit to New Delhi in October 2016.

NEXT STEPS

- Continuation of established cyber dialogues with Five Eyes partners, Australia, and China.

- Engagement with other priority countries on the margins of regional and multilateral cyber meetings.

- Australia will host the next Australia – New Zealand Cyber Security Dialogue in June 2017.

- Future ASEAN Regional Forum workshops are expected to feature regional desktop cyber incident response exercises.

ACTION 3:

Contribute to international cyber security capability and confidence.

OUTCOMES	PROGRESS TO DECEMBER 2016
• New Zealand capacity building helps to raise regional cyber capability, including through provision of assistance in the Pacific.	• NZ Police supported the Commonwealth Pacific Regional Cyber Crime Criminal Justice Training workshop in Tonga, March 2016. The workshop involved 10 Pacific Island countries and discussed common challenges inhibiting detection, investigations and prosecutions of cybercrime and related crime in the region. • New Zealand made a financial contribution to the ICT4Peace workshop for ASEAN developing countries on "cyber security cooperation, policy and diplomacy capacity building" in 2016. This funding helped to bring together officials from Cambodia, Laos, Myanmar and Vietnam and exposed them to a wide range of the issues involved in international cyber security discussions. • Discussions with Global Forum on Cyber Expertise (GFCE) secretariat and other members regarding possible future capacity building projects in the Pacific region, including at the first GFCE annual meeting in Washington, June 2016.
• New Zealand helps to build consensus on cyber confidence building measures in the Asia-Pacific region, including through the ASEAN Regional Forum.	• New Zealand has participated in ASEAN Regional Forum cyber security workshops focused on development of region-wide confidence building measures (e.g. sharing national policies, incident response exercises, lessons learnt, capacity building, research and analysis). • New Zealand and the Philippines will be the first co-chairs of an ASEAN Defence Ministers' Meeting Plus Expert Working Group on defence-related cyber security issues (2017-2020).
• 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.	• Inaugural cyber dialogue held with China in February 2016. The dialogue established policy and operational relationships, and ensured China is aware of New Zealand's approaches to major cyber security issues, both domestically and internationally.

NEXT STEPS

- Ongoing discussions with other donors/partners (led by World Bank and Interpol) on improved coordination of cyber security capacity building activities in the Pacific region.

- Ongoing discussion with New Zealand Aid Programme officials about the Pacific Regional Infrastructure Facility ICT work programme on cyber security.

- Ongoing discussions with private sector service providers on potential cyber security projects for Pacific Island countries.

ACTION 4:

Maximise the economic opportunities of cyberspace for New Zealand and New Zealanders.

OUTCOMES	PROGRESS TO DECEMBER 2016
• 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 key trading partners are pursued. • Engage with industry to understand, and consider how to address, any cybersecurity related impediments to trade.	• Engagement with the EU on the Network and Information Security (NIS) Directive, including with the New Zealand Embassy in Brussels and during NZ-EU Trade talks, March 2016. • Initial meeting with ICT services exporters to discuss the role of government in dealing with market access barriers arising from cyber security measures in export markets. • Discussions with US National Institute of Standards and Technology on cyber security workforce development (especially cyber training and retention), research and development initiatives, and cyber security credentials schemes.

NEXT STEPS

- Further building of relationships with key ICT exporters, with a focus on international regulatory challenges.
