Tēnā koutou, Tēnā koutou, Tēnā koutou katoa

Intro

- Welcome, and thank you all for coming to the launch of the 2019 New Zealand Cyber Security Strategy.
- I am so pleased to look around the room and recognise representatives from industry, academia, civil society and public service.
- I acknowledge my colleague Hon Andrew Little – thank you for joining us for breakfast during recess Andrew I know it's been a very busy time but I am pleased we are here together given the inter-connectedness of our work in cyber.
- It underlines, for me, one of the key principles of our new strategy: that "partnerships are crucial".
- I understand many of you directly contributed to developing the strategy - thank you for taking the time to help us shape it.

2019 strategy

- Government went out and engaged widely to hear what was important to the cyber security community, and, importantly, how we could help New Zealanders be confident and secure in the digital world.
- As a result, the 2019 Strategy emphasises the crucial role of individuals, businesses, community organisations and the private sector in achieving our vision of New Zealand being confident and secure in the digital world.

- Simply, we all have a role to play. All New Zealanders should be able to enjoy the benefits of greater connectedness in their homes and neighbourhoods, and this connectedness brings risks we need to address in partnership.

Internet way of life

- The internet is part of every New Zealander's life. We work, play, and stay connected with each other online. Even for the small part of the population not online, the critical services they rely on depend on internet connectivity.
- But with greater connection and dependence, comes greater exposure to cyber threats. That's why it's important that we focus on keeping New Zealand secure online.
- The past 12 months have underlined that cyber security is everyone's business, and why having a strategy is so important.

Increasing incidents

- Whether it be the compromise of the local Cryptopia cryptocurrency exchange, or the new global breaches reported every day, it's clear the threats we face from cyber space are diverse and growing.
- This is reflected by the numbers both from CERT NZ and the National Cyber Security Centre. Incidents reported to CERT NZ increased by 205% in 2018, with $14 million lost by individuals and businesses.
- The GCSB's National Cyber Security Centre recorded 347 incidents largely affecting organisations of national significance in the 2017 financial year. 39% of those incidents could be linked to state sponsored actors.

- Independent analysis estimates that CORTEX has reduced harm by $67million since 2016. 39% of those incidents could be linked to state sponsored actors.
- Clearly, malicious cyber actors are becoming more bold, brazen and disruptive. And as technology evolves these threats will grow and change.
- The Christchurch terror attacks and live streaming of abhorrent acts, demonstrate how the technologies that bring people together, can also be used for harm.
- New Zealand has to step up to confront these challenges. The 2019 Strategy will build on the government's existing work to secure New Zealanders.

Building awareness

- We are building awareness through CERT's *Cyber Smart* awareness campaigns. Last year the campaign had over 90 organisations partner with it on raising awareness, some of which are here this morning.

Other work we are doing includes:

- supporting research and development for cyber security through intergovernmental partnerships;
- the designation of the Director General of the GCSB as the Government Chief Information Security Officer; and
- advocating for a free, open and secure internet with our likeminded values partners.
- Following Cabinet approval last year the NCSC is on track to roll out its Malware Free Networks cyber defence capability to a broad cross section of New Zealand's organisations of national significance by June next year. And this year CERT is rolling out its new threat intelligence programme.

Many of you are involved in other cyber security initiatives – I hope we build on those foundations.

Strategy framework

- Turning to our 2019 New Zealand Cyber Security Strategy, it builds on the work I have just described. It provides a framework for achieving the Government's commitment to being a secure, connected digital nation.

- The strategy has four values:

Partnerships are crucial, because neither government nor the private sector can solve this problem on its own;

People are secure and human rights are respected online;

Economic growth is enhanced, as cyber security is an enabler of businesses remaining productive and profitable, and;

National security is protected.

- These values will define the approach to our work and support the development of a New Zealand that thrives in the digital age.

- The strategy has five priorities:

  - The first is **Cyber security aware and active citizens**: government will work with industry and civil society to build a culture of good security online. We need awareness to help our children communicate safely with us and their peers online, through to ensuring the boards of our largest companies know the impact data breaches can have on their bottom line and their customers' private information.
  - A **Strong and capable cyber security workforce and ecosystem** is needed, and an ecosystem of world class cyber security providers, capable of preventing, adapting to, and responding to threats.
  - We must be **Internationally active:** As the government works locally to create a cyber secure nation, we must work and talk with our international partners given the global nature of the threats. We will work with likeminded countries to advance our vision of a free, open and secure internet.
  - A **Resilient and responsive New Zealand**: building awareness is a great start, but we also have to ensure that we have the tools and know-how to resist cyber threats. The government will work to protect New Zealand's most important infrastructure systems, and help our networks to be resilient to major cyber incidents.
  - Finally, **Proactively tackle cybercrime**: as we become more connected, criminals seek to use those connections to exploit everyday New Zealanders. Often, they target our most vulnerable communities. We must ensure that we can investigate and prosecute cybercrime, providing justice for its victims.
    We will continue to implement New Zealand's action plan to address cybercrime and continue to work to fast track access to the Budapest Convention.

Funding

- The strategy has been allocated $8 million over the next four years to help achieve these goals. This is on top of $9.3 million increased funding for CERT NZ. We will work closely with the people here, and those who weren't able to make it this morning, as the government develops plans to implement these priorities.
- We will continue to work with individuals, businesses, community organisations and the private sector, in order to minimise harm and disruption, and make the most of technological advances.
- In a few moments the media will leave and I want to hear from you directly how we can do this and for us to share our progress, concerns and ideas.
- Thank you for attending this morning to help us create a confident, secure nation. Nga mihi.