The National Cyber Security Strategy 2015

What does mean it for InternetNZ & the Internet Community?

On 10 December 2015 Hon Amy Adams, Minister of Communications, launched the Government's new National Cyber Security Strategy (the Strategy), the Strategy's Action Plan and the Government's National Plan to Combat Cybercrime.

- Strategy: www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-december-2015.pdf
- Action plan: www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-action-plan-december-2015.pdf
- Cybercrime plan: www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-cybercrime-plan-december-2015.pdf

This short briefing lets you know:

a) what the Strategy is
b) how the Strategy is relevant to our strategic transformations and policy principles
c) what aspects of the Strategy we plan to engage government agencies on
d) any possible concerns we have identified.

Our quick read

1. The Strategy seeks to establish a national CERT. While there is little in the way of detail, this is an important step and something we have been calling for.
2. Partnerships are key. This is a stated principle of the Strategy and we will work to help make that principle a behavioural norm.
3. The Strategy itself has a strong national security focus and the most detailed aspects of the strategy appear to be those with a national security focus. We will work (with other interested parties) to ensure that the government does not overlook or de-prioritise the Internet security concerns of the rest of the Internet community.

What is the Strategy?

The Strategy sets out how the New Zealand Government thinks about Internet Security issues, how security issues link to our country's future economic prosperity and sets out a goal for New Zealand of being secure, resilient and prosperous online.

The Strategy is grounded in four principles: **partnership**, **economic growth**, **national security**, and **human rights.** The Strategy groups its efforts around these four goals (see below).

Source: the New Zealand National Cyber Security Strategy 2015

How is the Strategy relevant to us?

We are a voice for the Internet and a champion of the open and uncapturable Internet. The strategy is effectively about how to securely use the Internet for national prosperity. The content of the strategy, and its action plan is relevant to the following InternetNZ policy principles.

Internet governance should be determined by open, multi-stakeholder processes.
We need to make sure that everyone has had the chance to have an input into this process. All New Zealanders are affected by the way the Internet is governed and we look forward to expanding our working relationship with government agencies about Internet Governance.

Laws and policies should work with the architecture of the Internet, not against it.
This is especially true when it comes to international treaties or data collection. We are keen to work with officials to ensure that policy and legislative work under the strategy reflects the reality of the Internet. The aspects of the strategy that relate to this policy principle are also important to our policy principle that **technology changes quickly, so laws and policies should focus on activity.**

Human rights should apply online.
The Internet was built for humans, by humans. Our fundamental human rights do not reduce or disappear because we are using the Internet. Free speech online is still free speech. Online crime is still crime and the way the Government deals with it should not circumvent longstanding, protections and processes.

The Internet is nationally important infrastructure, so it should be protected.
The strategy has a number of components that relate to protecting and securing important 'information infrastructures'. We want to see more work on the areas of transparency, accountability and oversight to ensure that infrastructure protection efforts do not curb innovation.

You cannot have 'cyber security' without the Internet ('cyberspace' doesn't exist without the Internet) and we see this strategy as important context for our Internet Security workstream.

What we think

The Strategy's action plan has a lot of actions (17) in it, each with a number of bullet pointed projects or initiatives under the actions. We are not yet clear on the timing and prioritisation of these actions, or who is responsible for them. This will be a critical success factor for the Strategy, and experience tells us this is often one of the areas where government strategies can start to encounter delays and problems (especially if there is no funding allocated to action areas).

The Strategy's language and content is very National Security focussed with little comment or content relating to non-government, non-national security Internet issues. However, this is not surprising, nor is it necessarily a negative. It just means that we will have to work with other interested, non-Government organisations and groups to ensure that the Internet Security issues that matter the most to business and civil society are given appropriate priority and attention.

What do we plan to do about the Strategy?

We see a number of Action Points that we could potentially contribute to, as well as action points that we will be keeping an eye on.

We will be seeking further information about the following actions.

- We want to see a robust national CERT (Computer Emergency Response Team) that provides active incident response services across all of New Zealand's Internet community. We are working closely with the National Cyber Policy Office, and the NZITF, to make this a reality. [Resilience: Action 1]
- We will be seeking more information about the action to give additional support for ISPs. how the Government Communications Security Bureau will work with ISPs and what the proposed information flows and oversight will be. The recently publicised 'malware free networks' pilot[1] from the GCSB appears to be a potentially powerful tool in improving some networks' security. We are keen to hear more and are currently seeking briefing from the GCSB early in 2016. [Resilience: Action 2]
- We see a role for InternetNZ in championing the oversight of agencies' use of 'cyber tools', and the importance of rule of law. We also see opportunities to

[1] See the mention of malware free networks pilot under "Are ISPs involved in CORTEX?" on the CORTEX FAQ page here: http://www.gcsb.govt.nz/our-work/information-assurance/cortex-faqs/

improve Internet security across the country by open sourcing the tools that government agencies have created (where possible) so that the rest of New Zealand can better protect themselves. We will offer to work with government agencies to increase the availability and/or understanding of these tools. [Resilience: Action 3]

- We are particularly keen to work with the Government to ensure that when it considers how to "*Adapt New Zealand's policy and legislative settings for the digital age*", that this is done in a broad, inclusive and constructive manner. This will be important in adapting our laws for the Internet age, rather than simply giving law enforcement agencies more powers or new crimes to charge people with. [Cybercrime: Action 2]
- We are a trusted partner when the government represents New Zealand, and New Zealanders' interests in Internet Governance. We will continue to have a strong role to play in this area, and will align our representation in international fora where appropriate. [International Cooperation: Action 1]

Conclusions

The Government now has a new strategy, which includes the creation of a national CERT. After almost 2 years of effort refreshing the 2011 strategy, it is positive. We have been expressing the importance of a national CERT for close to a decade and it is great to see the Government taking action.

We see a number of opportunities for us to work with the Government, and others, to contribute to an Internet-connected New Zealand that is secure, resilient and prosperous. As a ConnectSmart partner, we will have a role as a fearless champion of the Internet, and ensuring that its benefits are not lost when discussing national or online security matters.

Given that the strategy is a 'cyber security' strategy written by a 'cyber policy' office, the term 'cyber' is used a lot in the document. We think that, in general, 'cyber' is sometimes used as a marketing badge, and it can be unclear what technical expertise or systems it relates to. For the most part, the strategy does a good job of ensuring that it maintains sufficient clarity about actions and areas of effect. However, in other areas it is too vague and limits our ability to both understand and effectively partner with the Government in delivery of the Action Plan.

About InternetNZ

A better world through a better Internet

InternetNZ is a voice, a helping hand and a guide to the Internet for all New Zealanders. It provides a voice for the Internet, to the government and the public; it gives a helping hand to the Internet community; and it provides a guide to those who seek knowledge, support or any other method of benefiting the Internet and its users.

For more information visit: https://internetnz.nz/about-us/internetnz-group