DEPARTMENT OF THE
PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

Cyber Security Strategy Annual Report for 2021/22

13/10/2022

Introduction

1. New Zealand's economic performance, the wellbeing of our citizens, and our connectedness with the rest of the world is ever more reliant on information communication technologies and an open, trusted internet. But the technologies that enable us to remain connected and that support the functioning of our economy and society also provide opportunities for those with criminal or hostile intentions.

2. Furthermore, COVID-19 forced a shift in the way New Zealanders work and live, increasing our dependence on tools that enable us to work, learn, and shop from home. This, too, has created new cyber threat vectors and risks for malicious actors to exploit.

Cyber security remains an important issue for New Zealand

3. Malicious cyber activity reported in New Zealand in 2021 largely matched international trends, with increases in both ransomware attacks and exploitation of internet-facing services and applications. In its 2021 Annual Report, the Government Communications Security Bureau (GCSB) noted that New Zealand organisations remain the target of persistent malicious cyber activity linked to state-sponsored actors.[1]

4. Both the GCSB's National Cyber Security Centre (NCSC) and CERT NZ reported marked increases in the volume of reports received in the last year, with the NCSC recording over 400 cyber security incidents affecting nationally significant organisations[2] and CERT NZ reporting 8,831 incidents[3] over the last reporting period.

5. These incidents can result in significant financial losses for affected business, with CERT NZ recording financial losses of over $15m as a result of incidents reported to them in 2021. Similarly, the NCSC estimates it has prevented over $100m in harm to nationally significant organisations through its prevention and resilience capabilities over the last year.

There is a broad programme of work being delivered under the Cyber Security Strategy

6. The Cyber Security Strategy 2019 (the Strategy) signals the Government's commitment to ensuring New Zealand is safe, resilient, and prosperous online. It outlines areas where government will prioritise action, and how the government will work together with individuals, businesses, and communities to ensure that New Zealand is confident and secure in the digital world.[4]

7. To ensure that New Zealanders can have confidence that the government is working towards this commitment, this report provides a summary of progress against the Strategy over the past year. It is important to note that lifting New Zealand's cyber security and resilience includes broad-based efforts alongside Strategy implementation, including through a range of individual agency initiatives and partnerships with the private sector.

8. The Strategy has five priority areas:
   - Cyber security aware and active citizens;
   - Resilient and responsive New Zealand;
   - Strong and capable cyber security workforce and ecosystem;
   - Proactively tackle cybercrime; and
   - Internationally active.

[1] https://www.gcsb.govt.nz/assets/GCSB-Annual-Reports/GCSB-Annual-Report-2021.pdf

[2] https://www.ncsc.govt.nz/assets/NCSC-Documents/2020-2021-NCSC-Cyber-Threat-Report.pdf

[3] https://www.cert.govt.nz/about/quarterly-report/2021-report-summary/

[4] More information on the Cyber Security Strategy 2019 can be found at https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf

9. The Strategy is underpinned by values that reflect New Zealand's unique place in the world, the government's commitments to New Zealanders, and the need for citizens and industry to work together with the government to build a safe and trusted internet. These values are:

- Partnerships are crucial;
- People are secure and human rights are respected online;
- Economic growth is enhanced; and
- National security is protected.

10. To support implementation of the Strategy, Budget 2019 allocated $2m per year for initiatives that seek to improve New Zealand's cyber security. This is in addition to significant individual agency funding, which is crucial to lifting the cyber security and resilience of New Zealand. Good progress was made during the 2021/22 year to commission and deliver a range of initiatives across the Strategy's five priority areas. A summary of key areas of work that contribute to delivery of the Strategy's objectives is provided below.

Implementation of the Cyber Security Strategy

Cyber security aware and active citizens

11. This priority area aims to build a culture in which New Zealanders can operate securely online and know what to do if something goes wrong. This includes initiatives targeted at building general skills and awareness of cyber issues across New Zealand.

12. Key activities supporting this priority focused on improving the accessibility and quality of CERT NZ awareness campaigns. This included translating CERT NZ resources into additional languages to improve accessibility of resources for groups such as Pasifika and vision-impaired communities.

13. It also included conducting market research on public cyber activity and hygiene habits to inform more effective public awareness campaigns on key cyber issues. This research has been reflected in initiatives such as the "Big Password Energy" campaign, targeting at-risk New Zealanders to influence them to lift the security of their online accounts.

Resilient and responsive New Zealand

14. This priority area is about ensuring that New Zealand can resist cyber threats, and that we have the tools and know-how to protect ourselves.

15. In November 2021, the NCSC facilitated a tabletop cyber security exercise in collaboration with industry. The objective of this was to improve responsiveness to cyber security incidents by testing existing plans, finding any gaps, and improving participants' understanding of their roles and responsibilities during an incident. Building on the lessons from that exercise, Strategy funding has been allocated in FY22/23 to develop a business case for an ongoing exercise programme.

16. In addition, a key government initiative to lift the resilience and responsiveness of New Zealand to cyber threats is the expansion of the NCSC's Malware Free Networks (MFN) capability, which is designed to strengthen New Zealand's cyber defence capabilities. MFN is a threat detection and disruption service that provides near real-time threat intelligence.

17. Significant investment has also been made in improving the resilience of both the public and private sectors as part of Budget 2022. Highlights include:

- $8m allocated to the NCSC to enhance its incident response capabilities;

- $12m to address cyber security risks at the Ministry of Justice, supporting courts and justice services to meet Protective Security Requirements and New Zealand Information Security Manual directives; and

- $7m to CERT NZ to fund its Cyber Smart Uplift project, which provides guidance to New Zealanders on how they can improve their cyber safety.

18. Cyber resilience is also a key theme that emerges through related sector strategies. The Ministry for Business, Innovation and Employment (MBIE) has led the development of a Digital Strategy for Aotearoa, which will set out the goals, priorities, and activities for the digital sector for the next 2 to 5 years, along with longer term outcomes out to 2032 and beyond. One of the pillars of the Digital Strategy is *Mahi Tika – Trust*, which notes that New Zealanders should feel safe and secure online as even the most innovative and future-focused digital businesses and government services can fail if users are not confident their data and privacy will be protected, or if users are concerned they are not safe online. Delivery of the initiatives under this pillar of the Digital Strategy will support stronger cyber security outcomes.

Strong and capable cyber security workforce and ecosystem

19. The purpose of this priority area is to ensure that New Zealand can rely on a strong cyber security workforce and sector, capable of preventing and responding to a range of cyber threats. This includes efforts targeted at building baseline skills, increasing the profile of cyber careers, and developing a diverse domestic cyber talent pipeline.

20. Recent activities have included research to better understand the cyber security workforce (including size, roles, demographics, and key skills gaps), which will inform the development and targeting of initiatives aimed at growing the domestic cyber security workforce and attracting international talent. A further project has delivered qualitative insights on opportunities for growing the domestic cyber security sector and better realising export growth.

21. Efforts to grow the cyber security workforce are also being advanced through the Digital Technologies Industry Transformation Plan (DTITP) – a long-term plan for the growth of the digital technologies sector being developed by government agencies in partnership with industry. The DTITP includes a focus on the growth of digital technologies workforce, as a critical enabler for the sector. This is a key mechanism for the delivery of initiatives to grow the cyber security workforce, as the skills challenges and opportunities faced by the cyber security sector share a number of commonalities with those experienced by the digital technologies sector more broadly.

Proactively tackle cybercrime

22. This priority area focuses on strengthening New Zealand's ability to proactively and collaboratively prevent, investigate, deter and respond to cybercrime, cyber-enabled crime and terrorist use of the internet.

23. Key initiatives under this priority area include a project to identify cross-cutting challenges for public safety and law enforcement in the digital age resulting from new and emerging technologies. A further project is designed to help New Zealand agencies identify where resources should be invested to address systemic vulnerabilities in New Zealand's frameworks for responding to online harm and preventing and disrupting online threats. These projects will help maximise the disruption of cybercrime, and deployment of intelligence and law enforcement tools to deliver criminal justice and national security outcomes.

24. As part of the decision in 2020 that New Zealand will accede to the Council of Europe Convention on Cybercrime (the Budapest Convention), the government agreed that officials should work with Māori to develop a mechanism to enable ongoing Māori involvement in New

Zealand's implementation of and participation in the Convention. Exploring a mechanism to enable this engagement has been a focus over the past year. In parallel, work is progressing on the draft Bill that enables accession to the Budapest Convention, before Cabinet considers introducing it to Parliament.

25. To further strengthen international cooperation in investigating and prosecuting cybercrime, New Zealand is also actively engaged in the United Nations process to negotiate a new international cybercrime treaty, which has included public engagement on New Zealand priorities in the negotiations (which can be found here).

Internationally active

26. This priority area is about advancing and protecting New Zealand's cyber interests through our international activity. This includes responding to malicious state-sponsored activity online, and cooperating with international partners to prevent and deter activity that threatens peace and security in cyberspace.

27. Government agencies have a significant programme of international engagement with bilateral partners and in regional and multilateral forums. This includes contributing to international cyber capacity-building efforts in the Pacific, as well as support to the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE). Agencies are also actively engaged in discussions at the United Nations on cyber security issues and the development of norms of responsible state behaviour online.

28. International activities funded by the Strategy have included New Zealand support for Ukraine's cyber resilience via a contribution to a USAID-delivered project. This responded to a request from Ukraine for New Zealand to support their cyber resilience and defence in the context of the Russian invasion.

29. New Zealand has contributed to the Women in International Security in Cyberspace Fellowship, which aims to support and upskill women participating in cyber discussions at the United Nations.

30. Support for cyber capacity-building in the Pacific is also provided via the Cyber Security Support to the Pacific Programme (CSSP), which is administered by the Ministry of Foreign Affairs and Trade (MFAT). This serves as a mechanism for New Zealand agencies provide cyber capacity building and support to identified cyber needs in the region. Since its establishment in 2019, the CSSP has enabled CERT NZ to provide peer support to Pacific governments; supported the establishment of a Samoan CERT and the development of Tokelau's Cyber Rules; and funded New Zealand Police to develop training materials on cyber security for Pacific Island police forces.

Looking ahead: Continuing to strengthen New Zealand's cyber resilience

31. Alongside the implementation of specific projects under the Cyber Security Strategy, work has continued to develop broader initiatives to lift the cyber security resilience of the public sector and the wider economy. Details of those initiatives already underway can be found in the *Budget 2022 Summary of Initiatives*, while further information on projects under development will become available as they move into consultation and implementation stages.