Aide-Mémoire

Health New Zealand
Te Whatu Ora

Deep Dive for Cyber Security

Due to MO:	6 March 2025	**Reference**	HNZ00080508
To:	Hon Simeon Brown, Minister of Health		
From:	Darren Douglass, Acting Chief Information Technology Officer		
Copy to:	n/a		
Security level:	Sensitive	**Priority**	Routine
Consulted	n/a		

Contact for further discussion (if required)			
Name	**Position**	**Phone**	**1st contact**
Darren Douglass	Acting Chief Information Technology Officer	s 9(2)(a)	
Sonny Taite	National Chief Information Security Officer	s 9(2)(a)	x

Attachments	
Appendix 1:	Environmental scan of the cyber security landscape (global examples)
Appendix 2:	Cyber Services Scorecard – February 2025
Appendix 3:	Cyber Security Uplift Programme – Services Delivered

Purpose

1. At your meeting with officials on Monday 17 February 2025 to discuss Health Infrastructure (HNZ00078388 refers), you requested further information about cyber security.
2. This aide-mémoire provides information on cyber security in Health New Zealand | Te Whatu Ora (Health NZ), including the threats we face, our readiness to respond to cyber-attacks, the outcomes delivered from targeted funding, and future priorities.

Executive Summary

3. The health sector is a high-risk target for cyber-attacks world-wide. In New Zealand, cyber-attacks against the health system have been steadily rising. Cyber security is a dynamic and evolving topic, new and emerging threats are a constant challenge.
4. The 2021 Waikato DHB ransomware attack and the associated disruption to clinical services was the catalyst for a five-year package funded in Budget 2021. The three-year cyber security uplift programme (CSU) concluded in June 2024, and we are now in the first of two maintenance years as part of the five-year investment.
5. The CSU programme delivered to scope and budget with an early focus on establishing a national security incident response capability. Combined with the deployment of a modern, intelligent national security system across all districts, we have been successful in detecting and disrupting many cyber-attacks that would previously have resulted in impacts to our health services or systems.
6. In addition to the CSU programme investments are being made from baseline funding to strengthen the most vulnerable parts of our health systems as part of lifecycle upgrade work. These investments are not impacted by proposed changes to the Health NZ Digital Services function.
7. S9(2)(f)(iv)

Background

Cyber Security Landscape

8. **The health sector is a high-risk target for cyber-attacks.** The health system is critical infrastructure for New Zealand, and the substantial amounts of sensitive data we hold makes us an attractive target. Top threats, consistent with our detection and response activities, include ongoing ransomware attack attempts, phishing and credential harvesting campaigns, and data breaches from identity theft and insider threats. This is a global issue, and not unique to New Zealand. Please see **Appendix 1** for some detailed examples.
9. **Our security operations detect high threat volumes.** The national security monitoring and alerting service was put into operation at the start of 2024. S9(2)(c) The National Security Operations Centre (NSOC) has a 15-minute response time for high severity

security events. This quick response time is needed as, after initial access to systems, the pace at which attackers move is now measured in minutes and hours rather than the previous days and weeks.

10. S9(2)(c)

11. **We face heightened risk due to deferred technical debt remediation.** Over time, technology systems accumulate 'technical debt,' which refers to the cost of additional rework caused by choosing expedient systems over better approaches. This cost and complexity introduce rigidities – necessary software updates, fixes, or improvements are delayed. Therefore, such outdated systems can be targeted by cyber attackers, particularly those that can no longer be updated or patched. S9(2)(c)

Incident Preparedness & Response

12. Cyber-attacks against the health system have been steadily rising. In the last 12 months, we activated our national security incident response team on more than 34 separate occasions, including in support of the wider sector, an increase from 21 activations in 2023. This early focus on response has resulted in detecting and disrupting several "Waikato-level" attacks that would have resulted in clinical service disruption.

13. The NSOC is responsible for the defence of our systems, networks and data, and has been in full service for one year. S9(2)(c)

Targeting investments to strengthen cyber security resilience

Cyber Security Uplift Programme

14. The May 2021 Waikato DHB Ransomware attack highlighted historical gaps in investment, security leadership, and cyber skills. A complex ecosystem and low cyber security maturity were highlighted by an independent review as areas needing improvement.

15. The CSU Programme was delivered from January 2022 to June 2024 with a budget of $66.1 million for 3 years and $48.4 million of operational funding for two 'out years' (to June 2026) to maintain improvements. Please see **Appendix 2**: Cyber Security Uplift Programme – Services Delivered.

16. The CSU Programme aimed to improve security leadership, response times, resilience, recovery, risk reduction and population awareness in New Zealand's health system. The programme established:

    a) Dedicated security leadership and the National Cyber Security function within Health NZ.

b) 24x7 security monitoring through the NSOC to prevent disruptions from ransomware attacks, and enhanced endpoint protection to safeguard critical systems against malware.

c) Technical Response (CSIRT) and Security Incident Management services ensuring swift response and recovery from incidents.

d) Services focused on identifying and mitigating vulnerabilities through a vulnerability management service.

e) Security assurance, consulting, and design services, ensuring that robust protections are in place, particularly for high-risk and critical systems, by embedding security by design best practices into the planning and design phases of projects, thus reducing the risk of breaches and system compromises.

f) National security awareness and education capability, which includes proactive measures such as continuous employee training to reduce phishing and credential harvesting risks.

g) A refreshed Health Information Security Framework (HISF) to address emerging threats, providing relevant guidance and tools for health sector organisations.

h) The Cyber Academy prototype providing a new pathway for recruits to enter the digital health workforce, to supplement critical skills gaps and create new pathways into the cyber workforce (including partnerships with external agencies).

17. One of the intended benefits of the CSU Programme was a better understanding of the threat landscape and our vulnerabilities. The Programme was never intended to address all gaps but knowing that these gaps exist means we can make informed decisions about how we respond. **Appendix 3** shows the Cyber Services Scorecard for February 2025.

Minimum Critical Cyber Security Improvement Programme

18. An additional $9.5 million was approved by the Chief Executive of Health NZ at the end of October 2024 to urgently address critical cyber security risks identified through a review of recent major cyber security incidents. The Minimum Critical Cyber security Improvement Programme (MCP) started building capacity in November 2024 and runs until the end of June 2025. It focuses on managing security risk across four areas:

a) **Data Protection** – S9(2)(c)
Development in this area for Health NZ is expected to benefit other government agencies and health organisations.

b) **Identity Management** – Strengthen identity management to reduce unauthorised access risks and improve system resilience.

c) **Cyber security Insurance Cover** – S9(2)(c)

d) **Privileged Access Management** – S9(2)(c)

Current and Future Issues

19. Cyber security is a dynamic and evolving topic. New and emerging threats are a constant challenge.

20. Investments are being made to strengthen the most vulnerable parts of our network as part of lifecycle upgrade work, and we are making incremental gains as opportunities present.

21. There is also a set of more strategic and systemic issues that we need to address, which are dependent on funding and are included in the DIP:

    a) S9(2)(f)(iv)

    b) S9(2)(f)(iv)

    c) **Emerging AI technologies raise significant data privacy and security concerns.** The unprotected database breach linked to the DeepSeek programme, along with its vulnerability to "jailbreaking" for cyber-crime and other harmful uses, has led to restrictions or bans in Australia, the United States, Taiwan, and Italy. European and South Korean regulators are investigating its data practices. Given the rapid pace of AI advancements, we must continuously monitor these developments and provide timely advice and guidance to ensure patient data remains secure and AI tools are used safely.

Funding

22. Improvements in cyber resilience have been delivered through time-bound funding for cyber security. Of the $51.6 million allocated to cyber security in 24/25 financial year, $17.9M is baseline expenditure, and $33.7 million is allocated to two timebound investment programmes:

    a) $9.5 million for the MCP, which expires in June 2025 and addresses high risk vulnerabilities identified through review of recent major cyber security incidents.

    b) $24.2 million for the final year of the CSU programme, which expires in June 2026 – allocated to security services, including the national security monitoring and alerting service.

23. These investments are not impacted by proposed changes to the Health NZ Digital Services function. Internal work is underway to secure permanent baseline funding to sustain these capabilities. A long-term funding commitment is essential to maintain and

improve protection and resilience.

24. There is a clear, evidence-based need to invest more in cyber security capability. A higher level of investment would target broader strategic and system issues that we need to address, and this is included as part of the DIP.

Next steps

25. The DIP assesses current digital infrastructure against potential investment priorities and opportunities to form a national view on the sequencing of investment over the next ten years (2025-2034). This is an opportunity to consider the long-term funding of cyber security capabilities and technical debt remediation.

26. S9(2)(f)(iv)

27. Health NZ will be including future funding requirements as part of preparing the DIP investment case (for external consideration) and operational budgets (for internal consideration).

28. Health NZ can provide additional information as required and is open to discuss any questions regarding the information in this aide-mémoire.

Appendix 1: Environmental scan of the cyber security landscape (global examples)

1. **External:** International incidents highlight the increasing impact of cyber-attacks on healthcare operations, patient safety, and workforce stability. The health sector remains a high-value target for financially motivated cyber-criminals and state-sponsored threat actors seeking to disrupt essential services.
2. **Australian Healthcare Attacks Impacting New Zealand**: Australian health providers continue to be targeted. A ransomware attack on a hearing clinic chain in Australia resulted in the theft of personal and health data, including information on New Zealand-based patients. In addition, supply chain attacks experienced in Australia often result in impacts to Health NZ suppliers because of their close relationship, or shared networks and systems.
3. **MediSecure Data Breach**: In April 2024, Australian electronic prescription provider, MediSecure, experienced a ransomware attack, exposing sensitive data of approximately 12.9 million individuals. The breach of personal and health information included prescription details. MediSecure's limited resources and planning was a primary factor in their failure to respond, leading to its voluntary administration in June 2024. This incident underscores the necessity for robust cyber security measures and adequate resourcing to manage potential breaches effectively.
4. **Long-Term Disruptions from Cyber-attacks**: The June 2024 ransomware attack on UK pathology provider Synnovis had lasting consequences. Staff went on strike in December due to stress from months of disrupted operations. The attack forced a return to manual processes, delayed results, and rescheduled surgeries.
5. S9(2)(c)

Appendix 2: Cyber Security Uplift Programme – Services Delivered

Following the Waikato Ransomware attack in 2021, Cabinet approved a five-year funding package, which included three years for the CSU Programme and an additional two years of operational funding to maintain improvements. The Programme focussed on 10 building blocks to improve cyber security maturity across 20 former DHBs and continued under Health NZ from July 2022.

- Total Investment Provided: $114.5 million over 5 years
- Total Funds Spent (FY22-FY24): $66.1 million
- Remaining Funds (FY25-FY26): $48.4 million
- S9(2)(j)

The table below outlines key achievements and deliverables of the CSU Programme, highlighting how each aspect has strengthened Health NZ's cyber security posture.

Programme Aspect	Description	What It Delivered
Dedicated Security Leadership	Establishment of dedicated security leadership within Health NZ	Created the National Cyber Security function to lead and coordinate cyber security efforts across the organisation.
National Security Operations Centre (NSOC) Service	24x7 security monitoring to prevent disruptions from ransomware and protect critical systems.	Implemented continuous monitoring and enhanced endpoint protection services across 20 Districts, reducing risks of ransomware and malware attacks.
CSIRT & Security Incident Management Services	Technical response teams and services to ensure swift incident response and recovery.	Provided rapid containment, investigation, and recovery from cyber security incidents, minimising operational disruptions.
Vulnerability Management Service	Service focused on identifying and mitigating system vulnerabilities.	Proactively identified, prioritised, and addressed vulnerabilities to reduce the attack surface for public network connected assets.
Security Assurance, Consulting, and Design Services	Embedding security by design into project planning and design phases for new systems.	Ensured that high-risk and critical systems had robust protections, reducing the risk of breaches and system compromises.

Programme Aspect	Description	What It Delivered
National Security Awareness and Education Service	A national capability focused on continuous security training for employees to reduce phishing risks.	Delivered ongoing security training, significantly lowering phishing and credential harvesting risks through awareness.
Health Information Security Framework (HISF)	A refreshed framework providing tools and guidance for addressing emerging cyber security threats in the health sector.	Updated the HISF to reflect current cyber security best practices, equipping health organisations with relevant guidance.
Cyber Academy Prototype	A new recruitment and training pathway for digital health roles, emphasising equity and diversity.	Launched the Cyber Academy, creating opportunities for diverse talent to enter the digital health workforce.

S9(2)(c)