Appendix 4: Sector Cyber Security Strategy and Roadmap

Executive Summary

1. The health sector is considered a critical national infrastructure. However, since the worldwide outbreak of COVID there has been a rapid increase in cyber security breaches internationally and nationally. The most consequential incident was the Waikato hospital ransomware event which occurred in May 2021 and resulted in a full systems outage of five hospitals.

2. During the COVID-19 outbreak we have also seen increased sharing of health information across internet connected systems, devices, and clinical services. This trend will only continue. As such, to protect sensitive information and ensure availability of healthcare services in an increasingly digital sector, there needs to be resources dedicated to building a strong cyber security foundation.

3. New Zealand's health sector does not have a consistent view of cyber security technologies and processes, and nor does it have enough experienced cyber security personnel to fully protect from cyber-attacks. Without change, it will not be safe to continue with the current pace of digitalisation of healthcare services in New Zealand. System reform provides the opportunity to take a stronger system wide approach to cyber security and address the most critical risks at pace.

4. In light of this, the Ministry of Health (the Ministry) has assessed the current level of cyber security maturity sector wide, including the Ministry's digital systems, to identify and prioritise areas for improvement. Maturity was rated on a scale of one to four[1] across 10 areas, hereinafter referred to as the "building blocks". Together, these building blocks, which have been defined with reference to the New Zealand Information Security Manual (NZISM) – a best-practice cyber security capability model – constitute a comprehensive cyber security strategy.

5. Interviews were held with all district health boards (DHBs) and the Ministry to score their current maturity as well as to capture commentary on risks, current state, and future plans. Note, that no interviews were held with the wider health network, ie, primary and community health providers. It is assumed that the DHBs are likely to have a higher level of maturity than these providers, therefore this strategy and roadmap defines the standard that all providers should meet.

6. s 6(a) [redacted]

- s 6(a) [redacted]

[1] A score of 1 indicates no, or very low maturity, while a score of 4 indicates very high maturity.

- s 6(a) [redacted]
- s 6(a) [redacted]
- s 6(a) [redacted]

7. The Ministry has considered several options to lift overall cyber security maturity to between 2.5 and 3.5 as follows. (A further summary of the outcomes of each of these options is included in Appendix 4):

   a. Option 1 "**Good practice standard**" (Recommended):

      - Uplifts maturity across the sector to an aggregate score of 3.5 out of 4 over three years.
      - Costs $10.0m in Capex over the first two years, and $24.2m annually in Opex from year one.

      The "good practice standard" option is recommended as it will enable the health system to successfully improve its risk posture at pace to a point where digital advances in health can be implemented securely; it will reduce the risk and impact of a successful cyber-attack to a more appropriate level; and assure the public that reasonable measures are in place to ensure their data is kept secure and cannot be stolen. Any options below "good practice standard" would only mitigate immediate risks and potentially leaves the sector open to sophisticated cyber attacks as experienced at Waikato DHB.

   b. Option 2 "***Minimum standard baseline***" (Not recommended):

      - Uplifts maturity across the sector to an aggregate score 3.0 out of 4 over two years.
      - Costs $11.0m in Capex over two years, and $18.2m annually in Opex.

      This would mitigate immediate risk and establish the basis on which to implement subsequent cybersecurity improvements but only on a regional basis rather than establishing a national capability. For example, this option will only fund regional security operations centres not an integrated national security operations centre. This option introduces additional risk such as the difficulty in recruiting key skills due to a perception that success will be difficult to insufficient funding.

   c. Option 3 "***Basic standard***" (Not recommended):

      - Uplifts maturity across the sector to an aggregate score 2.5 out of 4 over two years.
      - Costs $3.75m in Capex over two years, and $15.6m annually in Opex.

      The commitment to digital in the Health system reforms requires a corresponding level of investment in Cyber security protections. This option will not sufficiently mitigate the ongoing risks of a cyber-attack such as the one Waikato DHB recently experienced. It would be very difficult to recruit key skills due to insufficient funding and a perception we are not serious about security.

8. As stated above any options below “good practice standard” would only mitigate immediate risks and potentially leaves the sector open to sophisticated cyber attacks as experienced at Waikato DHB. The transition to the target state will be over three years, reflecting the complexity of the current environment and the need to iteratively improve workforce, process and technology capability maturity at national, regional and organisational levels.

9. A cybersecurity roadmap to implement the good practice standard will remediate the most serious risks first and subsequently system wide cybersecurity improvements. It will:
    a. Build a set of core cyber security capabilities for hospitals, primary and community services in each region.
    b. Enable the health sector to successfully improve its risk posture to a point where digital advances in health can be implemented securely, with reduced and acceptable risk of compromise.
    c. Reduce the almost certain likelihood of another successful cyber-attack to a more appropriate level.
    d. Provide a basis on which to implement subsequent cyber security improvements funded from baseline budgets beyond the three year investment horizon proposed in this paper.
    e. Meet the expectation of the public that reasonable measures are in place to ensure their patient data is kept secure and cannot be stolen.
    f. Wherever possible leverage the use of cloud technologies, including “as a service” security software, as a method of quick means of improving cybersecurity across the health sector.

10. The prioritised list capabilities on the roadmap also conforms with government advice from NCSC and CERTNZ Critical Controls. Specifically, the roadmap will implement the following CERTNZ Critical Controls:
    a. Patch your software and systems (vulnerability management)
    b. Secure internet-exposed services (external network services)
    c. Configure logging and alerting including automated detection and response (national SOC/SEIM)
    d. Implement multi-factor authentication and verification (Identity and access management)
    e. Implement network segmentation (internal network security)

11. The Ministry is also recommending a change to the health sector’s traditional cyber security operating model whereby cyber security resources are exclusively allocated within the Ministry or DHB’s (including their shared service agencies). The proposed new operating model shares resources and capability across the sector. For example, a new CISO roles would be established at a national level to support proposed regional CISO roles and primary and community providers. Additionally, regional cyber security operations teams will provide the primary sector with specific security operations capabilities e.g. incident response.

Threat Landscape

Healthcare providers are increasingly being targeted by cyber criminals

12. Healthcare is one of the most targeted sectors globally and the threat environment is constantly evolving with more, and increasingly sophisticated, attacks. Personal Health Information (PHI) is highly prized by those who want to sell it or use it to ransom healthcare providers. The New Zealand health sector has seen a rapid increase in cyber-related incidents. Some of these incidents stem from poor practices, whereas other are a result of global cybercrime, somewhat driven off the back of the COVID-19 pandemic response. A list of the most significant events in the health sector is shown below:

What Happened	Why It Happened
s 6(a) [redacted]	

Rapid movement towards a digital, connected and always on environment

13. Increasing the care of our patients outside the hospital using digitally enabled patient services is a key part of system reform. With the digital 'new normal' comes the responsibility of ensuring those systems, services, and data remain safe and secure whilst maintaining privacy.

14. The acceleration of digital and cloud solutions provides opportunities to implement "secure by design" solutions. However, years of under investment in health information systems in New Zealand means the complex and aging technology landscape provides challenges to safely and quickly moving to use cloud services while the increased demand for "access anywhere" demand a high level of cyber security capability and maturity. Sharing information across health networks and internet connected devices in and outside hospitals, is increasingly becoming the status quo. Whilst this leads to better patient care and health outcomes, it introduces more risk into an environment that is far from being resilient to cyber threats.

15. A primary business problem is that the health sector does not have consistent, comprehensive approach to cyber security technologies, processes, and people trained and experienced in cyber security. To fully protect the sector from cyber-attacks and enable the new digital journey, this must be addressed.

16. The sector must adopt a holistic cyber security approach based on key cyber security building blocks to enable cyber resilience and to enable a borderless, integrated regional health system that allows care to delivered in different ways and support reduced demand on acute beds and resources.

Current State of the Health Sector

17. s 6(a) [redacted]

s 6(a) [redacted]

s 6(a) [redacted]

s 6(a) [redacted]

s 6(a) [redacted]

s 6(a)

[redacted]

s 6(a)

[redacted]

s 6(a)

[redacted]

s 6(a) [redacted]

How do we address the current lack of maturity?

18. The Ministry's review shows that the health sector is below the expected baseline with regards to cyber security. To address this, the Ministry has identified 10 building blocks which make up a comprehensive cyber security strategy. In addition to this, the Ministry has also developed a roadmap of proposed initiatives for implementation. The proposed funding options have varying levels of uplift across these building blocks

19. The goal of the strategy is to lift overall cyber security maturity to 3.5 in the key areas of risk (people and capability, network security, end-point security, compliance to standards and SEIM).

20. Regardless of which of the three options are supported, there will need to be investment over multiple years. This is because the health sector is starting from a low maturity baseline. The use of cloud and "as a service" security technology will enable a more rapid increase maturity.

    The increase in maturity across the functional areas is shown below:

Option 1 **"good practice standard"**		**Dedicated and experienced security leadership**	**Security standard and assurance**	**Security Resourcing and Education**	**Identity and Access Management**	**Cyber Incident Response Plan, Partner and Capability**	**Internal Network Security**	**Advanced Web Application Firewalls**	**Endpoint Security**	**External and Internal Vulnerability Management**	**Security Event and Incident Management Systems (including incident response)**
Additional Capability/uplift	National	1 new National CISO plus 1 new Primary Sector CISO 2 new FTE	s 9(2)(j)								
	Northern	None									
	Te Manawa Taki	1 new CISO 4 new FTE									
	Central	1 new CISO 4 new FTE									
	South Island	1 new CISO 4 new FTE									
Future state capability maturity (increase in maturity score from current state)		s 6(a)									

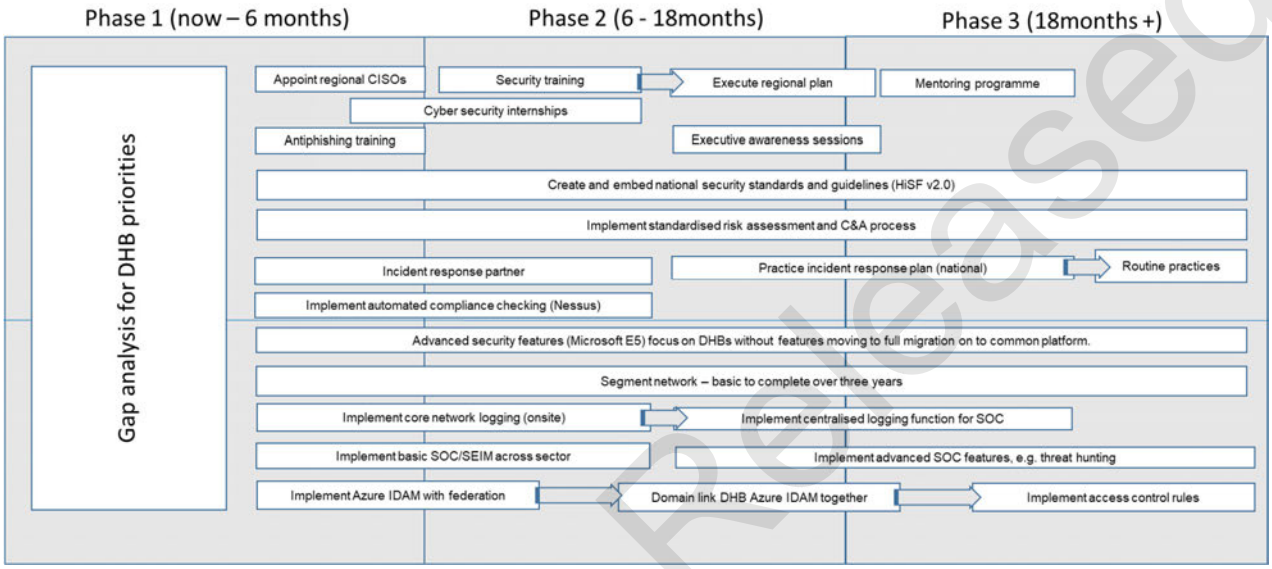
21. The phasing of capability uplift across the ten building blocks and the associated costs is shown below:

Financial Year	Opex / Capex Split	Total	Project Management	Dedicated and experienced security leadership	Security standard and assurance	Security Resourcing and Education	Identity and Access Management*	Cyber Incident Response Plan, Partner and Capability	Internal Network Security	Advanced Web Application Firewalls	Endpoint Security	External and Internal Vulnerability Management	Security Event and Incident Management Systems (including incident response)
Year 1	Capex	$2.530m	s 9(2)(j)	[redacted]									
	Opex	$19.175m											
Year 2	Capex	$7.470m											
	Opex	$24.2m											
Year 3	Capex	-											
	Opex	$24.2m											

* costs included in Endpoint Security

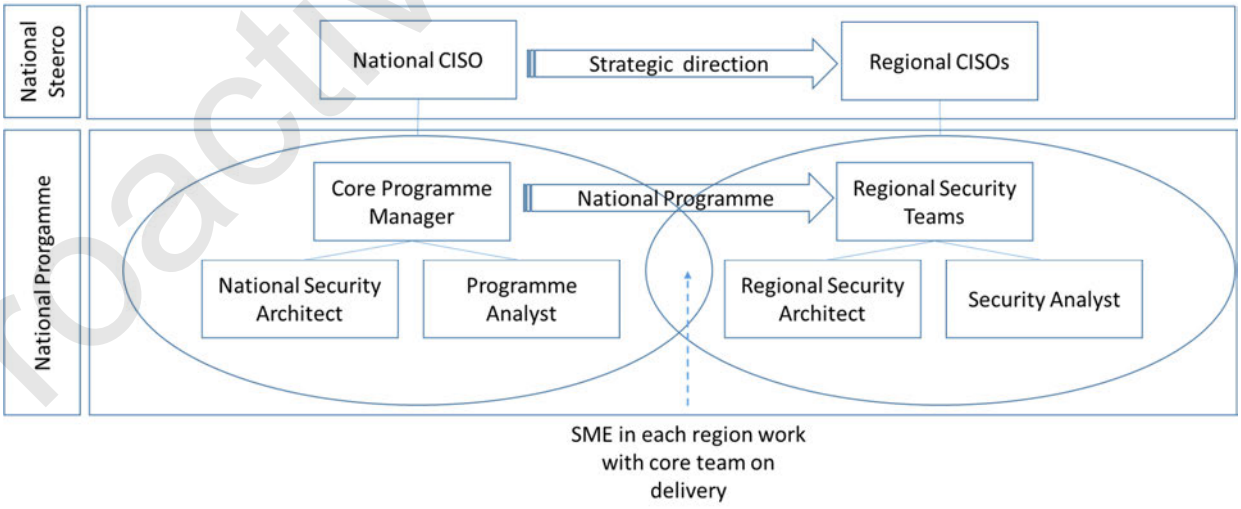
Roadmap

22. The security programme will be delivered over three years. A concept roadmap outlining key stages of delivery is outlined in the diagram below:



Delivery structure

23. Delivery of the cyber security roadmap will be centrally led (including specified standards and oversight, and leveraging subject matter expertise in the sector) but regionally and locally delivered as outlined in the diagram below:



24. Key points to note are:

- Delivery of the cybersecurity roadmap will be managed in line with the key principles from Managing Successful Programmes (MSP) and incorporate controls and processes, including for risk, issue and dependency management and quality assurance.
- Procurement activities will align with the Ministry of Health procurement policy, which sets out the framework for undertaking procurement in a way that encompasses value for money, fairness and transparency.
- Governance of the cyber security roadmap delivery will be undertaken by the Cyber Security National Steering Committee. Membership will include:
    - National CISO
    - Regional CISO's (once in place)
    - Ministry and Sector executive representatives
    - Cross Government Agencies (NCSC, GCDO)
- Delivery of the roadmap will be managed as directed by the Cyber Security National Steering Committee. Visibility and transparency of investment decisions and value realisation will be provided to the Capability Uplift Portfolio Board.
- The National CISO will be the Senior Responsible Owner for the cybersecurity roadmap delivery, with the ownership and leadership for capability delivery sitting with regional CISOs.
- Regions that already have advanced security capabilities, such as the Northern region, will support the deployment of capability into regions with less maturity, in line with direction from the SRO.
- Where regions do not have cybersecurity expertise this will be co-funded out of the national cybersecurity roadmap delivery budget.

New security operating model

25. In addition to the proposed investment in people and technology, a new operating model is proposed:

26. The proposed operating model is a matrix model with investment in a primary sector security leader to undertake a functional security role across all regions. Specifically, the role will provide:
    - National security leadership activities in the primary sector

- Governance and enforcement and update of national policies, standards, and guidelines
- Primary sector education and awareness
- National sector and cross-government liaison
- Assurance checks on key NGOs/primary health organisations.
- Undertake routine compliance

27. Other cross-functional technical security capability will be resourced out of each region for essential technical functions such as:
    - Reviewing threat intelligence from NCSC or other providers to ensure the health sector is not exposed
    - Conducting routine security tests or looking for possible security breaches
    - Incident response capability for responding to major events
28. This new model is proposed to enable the sector to build centres of excellence and enables the primary sector members to benefit from the above investments.

Conclusion

29. In the context of increasing cyberattacks, increasing use of digital in the sector, and increased concerns from patients about the security and privacy of their data, cyber maturity is currently not adequate. As we have seen in recent months in New Zealand, cyber security incidents can have a material impact on the delivery of healthcare to New Zealanders. The current cyber security risk posture needs to be addressed.

30. s 6(a) [redacted]

31. The health sector also needs a solid and robust cyber security framework to take advantage of advanced digital technologies because these systems predominately operate over the internet and collect and exchange large amounts of patient data.

32. This paper has considered options to address the shortfall of capability and recommends that the sector achieve a good practice standard with urgency. Implementation of a cybersecurity roadmap over three years is proposed.

33. s 6(a) [redacted]

- s 6(a) [redacted]
- [redacted]

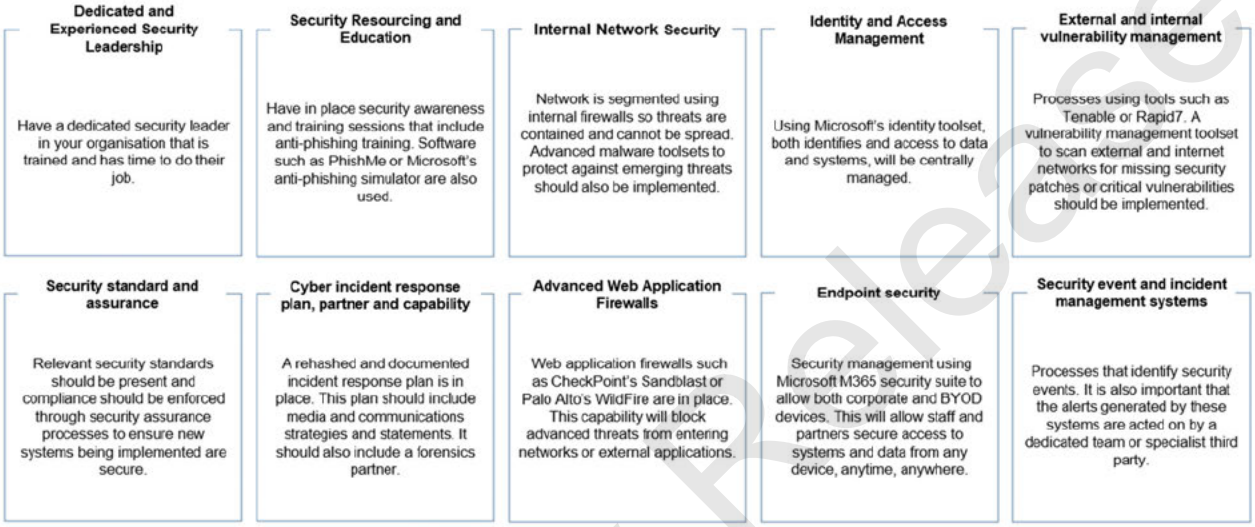
34. Without adequate investment in security, privacy and security breaches will continue and public trust will be eroded.

Appendices

Appendix 1: Building blocks

The building blocks are outlined below and are built on the Health Information Security Framework which meets government expectations, ie, NZ SIS Protective Security Requirements and GCSB New Zealand Information Security Manual.

These core building blocks are shown below:



All DHBs were surveyed and their maturity across the building blocks was determined. s 6(a) [redacted]

s 6(a)

Appendix 3 – Analysis of the other options

Option 2 – minimum required baseline- A planned uplift across the sector to a cyber security of 3.0 out of 4 and will take 2 years to implement.

Option 2 **"min standard baseline"**		Dedicated and experienced security leadership	Security standard and assurance	Security Resourcing and Education	Identity and Access Management	Cyber Incident Response Plan, Partner and Capability	Internal Network Security	Advanced Web Application Firewalls	Endpoint Security	External and Internal Vulnerability Management	Security Event and Incident Management Systems (including incident response)
Option 2 Additional Capability/uplift (Cyber security maturity = 3)	National	1 new National CISO plus 1 new Primary Sector CISO 2 new FTE	s 9(2)(j)								
	Northern (3)	None									
	Te Manawa Taki (3)	1 new CISO 2 new FTE									
	Central (3)	1 new CISO 2 new FTE									

	South Island (3)	1 new CISO 2 new FTE									s 9(2)(b)(ii) [redacted]
Future state = X Increase In Security Maturity Score = (X)	s 6(a) [redacted]										
Capex ($11m) includes 750k project costs Opex ($18.2m annually)	s 9(2)(j) [redacted]										

Option 3 - Basic - A planned uplift across the sector to a cyber security of 2.5 out of 4 and will take one year to implement but leaves the sector exposed to the ongoing risks of a cyber-attack akin to the one Waikato DHB experienced.

Option 3 **"basic"**		**Dedicated and experienced security leadership**	**Security standard and assurance**	**Security Resourcing and Education**	**Identity and Access Management**	**Cyber Incident Response Plan, Partner and Capability**	**Internal Network Security**	**Advanced Web Application Firewalls**	**Endpoint Security**	**External and Internal Vulnerability Management**	**Security Event and Incident Management Systems (including incident response)**
Option 3 Additional Capability/uplift (Cyber security maturity =2.5)	National	1 new National CISO plus 1 new Primary Sector CISO 2 new FTE	s 6(a) [redacted]								

								s 6(a)			
		Northern (3)	None								s 6(a)
		Te Manawa Taki (3)	1 new CISO 1 new FTE								
		Central (3)	1 new CISO 1 new FTE								
		South Island (3)	1 new CISO 1 new FTE								
Future state = X Increase In Security Maturity Score = (X)		s 6(a)									
Capex ($3.75m) includes project costs Opex ($15.6m annually)		s 9(2)(j)									

The Ministry has reviewed the three options against a fixed list of criteria shown in the table below:

Assessment	Description	Option 1 "good practice standard"	Option 2 *"min standard baseline"*	Option 3 *"basic"*
Cost	Is the cost of the option moderate or significant?	Acceptable	Acceptable	Cheapest
Change	Is this option able to meet the ever-changing requirements/threats, i.e., is it future proof?	Yes	Partial	No
Compliance	Does this option meet the Health Information Security Framework requirements, i.e., does it lift Sector cyber maturity to acceptable baseline?	Yes	Yes	Partial
Continuity (cyber resilience)	Does this option give the sector enough cyber resiliency to withstand a major event?	Yes	Partial	No
Coverage	Does this option meet all essential/missing cyber security controls?	Yes	Yes	No
Mitigates immediate security risks	Does this solution address the areas of greatest concern?	Yes	Yes	Partial
Enables digital transformation	Does this option support and enable the digital transformation occurring within the sector?	Yes	No	No

Appendix 4:

This table provides a high-level summary view of the outcomes at each maturity point considered in this paper.

Building blocks	Maturity level		
	2.5	3.0	3.5
Cyber security staff *"Well trained and experience drivers lead to fewer crashes and following of the rules".*	A limited increase in the number of cyber security staff which will help manage current, day to day DHB security workload	Increased cyber security staff with regional cyber leaders who can undertake not only current but future day to day DHB security workload	Enough cybersecurity staff in each region to manage current and future workloads including the primary sector in terms of incident response and basic systems assurance activities.
Standards *"A road code for security that people need to follow to avoid accidents or injury."*	Basic common standards will be available to each region who will have to self-manage DHB adherence to the standard	Training on the use of common standards including the deployment of limited automated compliance which will drive increased DHB compliance and consistency of security standards	Implementation of automated compliance tools freeing up cybersecurity staff to work with health sector on how to manage cybersecurity risks. Implementation of cybersecurity tools to simulate security breaches by checking the health sector network for possible security weaknesses.
Education *"Ongoing driver education makes for better drivers"*	Basic security education to address immediate DHB risks	Improved staff cybersecurity education using simulation tools such as phishing, which is presently the most common method of security compromise	Online security education, including simulations to staff are educated on the latest security threats, including how to react, report and identify potential security threats.
Access management *"A standard driver license you can use while on holiday"*	Basic access management solution to allow DBH staff with shared access to external applications	Single sign on capability to a range of systems using one identity across the health sector	Advantaged single sign-on capability using one-logon to a range of shared health sector systems to staff, contractor and trusted third parties.

Building blocks	Maturity level		
	2.5	3.0	3.5
Internal network security and segmentation *"Medium barriers separates traffic and also motorways from domestic roads"*	Basic internal networks separation between corporate network and medical networks in public hospitals	Increased network separation in public hospitals with additional security features to stop security threats infecting the whole health sector network	Advanced internal networks separation between network functions using advanced firewalling features across the health sector. Upgrade of the Connected Health upgrade to improve access with additional security
External security services *"off-road protection that protects the driver "*	Basic external security services to protect against common security threats	Advanced security features for external security services that protect against advanced security threats.	Advanced cloud "as a service" ever green security services that enable cloud services to be securely and easily implemented covering off new and emerging threats, e.g. DDOS, Ransomware, etc.
Endpoint security protection *"Robust tires, brakes and suspension allows for safe driving on and off road."*	Advanced endpoint security protection for DHB devices	Advanced security features for laptops and mobile devices so DHB staff, contractors and third parties can securely access health sector systems.	The ability for staff to use any device, anywhere with the correct level of security to mitigate any "off network" security threats. The ability to allow health sector staff to securely exchange data and also monitor for and prevent loss of sensitive data.
Vulnerability management *"Warrant of fitness toolset to highlight weaknesses that could result in failure or an incident"*	Basic security vulnerability management targeted at critical systems	Basic security vulnerability management targeted at critical systems and external websites	Advanced security vulnerability management and security scanning for both internal, external and medical devices to proactively identify security vulnerabilities.

Building blocks	Maturity level		
	2.5	3.0	3.5
Security Operations Centre *"Speed cameras to highlight drivers who are speeding and might crash or endanger other drivers."*	Limited local security with a basic security logging and event management system	The implementation of a national system to collect, analyse and respond to security threats but with regional teams. This allows regional security to see threats affecting the whole sector and take proactive action locally to thwart possible security breaches.	A unified national system with a national team to detect and respond to security incidents before they become large, including automation to process common security threats without the need for manual intervention.
Incident Response *"Roadside assistance. It helps you get back up and running quickly. It's also cheaper if you purchase it in advance."*	Limited incident capability through cybersecurity insurance partner.	Pre-arranged access to experienced security responders with up-to-date skills so cyber incidents are dealt with quickly and do not become large, public and long-term incidents.	On top of access to experienced incident responders there will be an annual sector wide simulation to test the sector is able to quickly react to large, public incidents correctly.