Memorandum

Update on operation SONIC

Date due to MO:	20 September 2019	**Action required by:**	<N/A>
Security level:	[redacted]	**Health Report number:**	20191826
To:	Hon Dr. David Clark, Minister of Health		

Contact for telephone discussion

Name	Position	Telephone
Dr. Ashley Bloomfield	Director-General of Health	s 9(2)(a)
Shayne Hunter	Deputy Director-General, Data and Digital	s 9(2)(a)
Darren Douglass	Group Manager, Digital Strategy & Investment, Data and Digital	s 9(2)(a)
David Metcalfe	IT Security Manager, National Digital Services, Data and Digital (technical SME)	s 9(2)(a)

Action for Private Secretaries

N/A

Date dispatched to MO:

Update on operation SONIC

Purpose of report

1. This report provides an update to the previous Health Report (20191772) regarding the cyber security breach at Tū Ora Compass Health (Tū Ora) Primary Health Organisation (PHO).

Current Status

2. The investigation continues and there remains no conclusive evidence whether information was copied and extracted. However, it is considered highly likely given past experience with cyber-crime.

3. Tū Ora have analysed the information to determine the potential extent of the exposed data. There is no change to what has been previously advised. This analysis is informing the response and communications plans. Key stakeholders such as the Tū Ora Board and customer District Health Board (DHB) CIOs and CEOs have been briefed.

4. Tū Ora and the Ministry of Health (the Ministry) continue to work on communications and response activities. The response plan will ensure that support for the public is in place and the potential broader system impact has been considered before information about the incident is disclosed. The response plan is being prepared with input from central agencies and the Privacy Commissioner.

5. It is intended to submit a response plan to the Official's Committee for Domestic and External Security Coordination (ODESC) for consideration by 26 September 2019. ODESC will provide advice to Ministers and this will include considerations around public disclosure and timing.

6. The Ministry, supported by the National Cyber Security Centre (NCSC, part of the Government Security Communications Bureau), has commenced assurance activities across other critical health organisations. The Ministry has had input from the Government Chief Digital Officer (GCDO) and Government Chief Information Security Officer (GCISO) to ensure a consistent approach across the system.

Response plan updates and next steps:

7. Updates on key activities in the response plan are as follows (Appendix A outlines more detail on the full response plan).

Communication and support to affected individuals

8. The Ministry continues to work closely with Tū Ora in preparing communications, reactive communications material and advice for affected individuals in the event that the incident is proactively disclosed. Reactive messages have been prepared to respond in the event of an unplanned disclosure of the breach.

9. The PHO and the Ministry are balancing the need to ensure the right information is available to those affected about increased risk, weighted against our actions increasing the risk of further attacks and the harm disclosure will cause to individuals.

10. A meeting was held on 18 September 2019 between the Ministry of Health, Computer Emergency Response Team (CERT NZ), NCSC, DPMC, and NZ Police, to discuss potential malicious uses of the information by cyber criminals if disclosed. This was used as input to the communications planning.

Tū Ora assurance

11. Officials continue to investigate the extent and scale of the breach; this work is expected to conclude by 27 September 2019. However, as advised previously, due to a lack of available information from Tū Ora's environment it is unlikely to be possible to confirm whether data has been accessed.

12. The Ministry will require Tū Ora to engage an independent third party to conduct security assurance activities on their new website environment, and other externally facing systems, to validate that they are secure. This is expected to occur in October once Tū Ora have completed preparations to respond to a public disclosure.

13. It should be noted that the Ministry's authority to require health sector agencies to complete independent assessments of their environments is limited in the short term, due to the contracting arrangements. s 9(2)(f)(iv) [redacted]

14. s 9(2)(h) [redacted]

Immediate health system actions

15. Further actions are planned to proceed as quickly as possible, noting it will require extra resources and the Ministry is looking at ways of funding them. The key immediate steps over the next three weeks include:

    a. Seeking confirmation of incident containment

    b. Confirmation of the data disclosure risk

    c. Communications plan and an analysis on disclosure risks

Request for health sector assurance

16. The Ministry requested on 19 September 2019 that DHBs, PHOs and health shared service agencies provide assurance regarding the security of their externally facing systems. Responses are required by 4 October 2019.

Independent security assessments

17. The Ministry is meeting with DHB, PHO and shared service agency CIOs on 20 September 2019 to notify them of the intent to conduct reviews of their externally facing systems for security vulnerabilities.

18. The NCSC will conduct analysis of PHO websites to determine if they are vulnerable to the same exploits as the Tū Ora incident. This is expected to start on 23 September 2019 and take at least four weeks to complete.

19. Depending on availability of the third-party security organisations, assessments of the prioritised health organisations are expected to commence in early October and take

three months to complete. Timing around remediation of the findings will depend on the technical complexity to resolve and the availability of budget and resources in the health organisation.

Longer term actions

20. s 9(2)(f)(iv) [redacted]

Response Plan next steps

21. The Ministry will provide an update the week of 30 September on the status of the response plan and incident.

Recommendations

The Ministry recommends that you:

a) **Forward** a copy of this report to the following Ministers:

- Rt Hon Jacinda Ardern, Prime Minister
- Hon Kris Faafoi, Minister of Broadcasting, Communications and Digital Media
- Hon Chris Hipkins, Minister for State Services Commission
- Hon Andrew Little, Minister Responsible for Government Communications Security Bureau

Dr. Ashley Bloomfield
Director-General of Health

Hon Dr David Clark
Minister of Health
Date:

ENDS.

Appendix A – Response Plan

Dated	19 September 2019	**Time**	2100	**Operational period**	*September 2019 – December 2020*
Situation summary	Current evidence suggests that Tū Ora Compass Health (Tū Ora) was compromised four times between July 2016 and August 2019 by multiple external threat actors. The exploits have been mitigated to prevent further risk. The exploits allowed the threat actors to access their Internet facing web server, which also contained large amounts of personally identifiable information with health context. It also contained administrative level credentials for the other systems in the Tū Ora network. The data was not used to support clinical care, so from a clinical perspective there is low risk. However, there is the potential that malicious actors could cause harm through cybercrime including phishing, spear phishing, scams, identity theft, and blackmail. There is no evidence of data being exfiltrated from Tū Ora but it is highly likely that this has occurred. The investigation into the size and scale of the breach is ongoing. The scale and the nature of this incident has the potential to have an impact on the broader public system. This response plan considers both the Tū Ora incident, and the potential impact on the broader system.				
Aim of response / end state	s 9(2)(g)(i) [redacted] The aim of the response is to: • minimise the harm to affected individuals • confirm the risk has been contained and to validate that Tū Ora security practices are appropriate • respond to the incident in a way that does not undermine public confidence in the broader system and the New Zealand government, and ensure support is in place for the impacted individuals. Given it is probable that these technical security shortcomings exist in other organisations across the health sector, this response will also seek to provide assurance that major and critical health sector organisations security practices are appropriate. Key objectives include: • Establish communication plans for reactive and proactive disclosures and define key 'go/no-go' criteria and decision points.				

	• Ensure that support for the public is in place. • Confirm the size and scale of the breach, to the extent reasonably possible. • Ensure the broader system impacts are understood and mitigation response strategies are in place. • Beyond initial containment measures, undertake medium-to-long-term strategies to review and increase cyber security maturity across the health sector.
Key risks	• The harm disclosure will have on vulnerable individuals who will be acutely concerned about the loss of their health information • Exposure goes beyond what has already been identified, where additional systems or files in Tū Ora or other organisations may have been compromised further expanding the impact of the incident. • Unplanned disclosure before Tū Ora has released their statement. This may result in confusion to the public, as they may not have access to the answers they want around the types of information accessed, if they are affected, etc. This could cause stress and concern to the public. • s 9(2)(g)(i) [redacted] • Increased phishing or scams, blackmail, or disclosure of information. Attacks like phishing and scams will likely occur with just the knowledge of the incident, even if the data itself was not exposed. • Health organisations are not able to react fast enough and are exposed if there is increased cyber activity.
Contractual relationship with PHOs	A Primary Health Organisation (PHO) is not a government agency. A PHO is contracted by a District Health Board (DHB) under a “PHO Services Agreement”. That agreement includes in Schedule B1, Section 9: “*preserve and protect the safety, security and confidentiality of the Records*” The DHB is contracted by the Ministry under a Crown Funding Agreement which has an operational policy framework attached. This framework includes the following under section 13.13: *Ensure that contracts entered into via the DHB funding arm include a requirement to observe privacy and security standards (as specified in 13.11.3).* Section 13.11.e is as follows: *Implement a security maturity work-programme aligned with the Health Information Security Framework and the New Zealand Information Security Manual. Key goals within the development of this work-programme should be:* *i. identifying the Board and/or Tier 1-3 leadership positions within the DHB that will deliver its mandated security governance obligations;*

	ii. defining the security oversight responsibilities that will be fulfilled by these identified DHB leaders; *iii. to maintain appropriate ICT security assurance processes for both the upgrading of existing capabilities, and the introduction into service of new ones;* *iv. to embed a "security-by-design" process within the DHB's ICT procurement [and by extension, detailed business cases] processes;* *v. to have a formalised cloud risk assessment process; and* vi. *to identify and catalogue security professional capability gaps within the DHB's ICT operations work-force.*

Immediate Actions

The following table outlines the key actions to be undertaken with urgency, to the extent reasonably possible given the circumstances. The immediate actions are planned to proceed as quickly as possible, subject to capacity constraints. These actions are not currently included in approved budgets.

Objectives / lines of effort / phases / activity	**Sub-phase**	**Tasks / Actions**	**Who is responsible for leading**	**Target timeframe**	**Comments (**including timeframes / milestones)
Assurance – Tū Ora					
Confirmation of containment	N/A	• Continue the investigation to determine if the incident is contained. • Attempt to determine conclusively if the data was accessed, or other systems in the Tū Ora environment were also accessed. • Determine if there is a possibility the Tū Ora systems could have accessed information or systems in other organisations.	NCSC	27 Sept 2019	No evidence to date of ongoing compromise. Limited information available in the Tū Ora environment to determine further data or system access.
Confirmation of data disclosure risk	N/A	The type of datasets that were potentially (or likely) accessed as a result of the security	Tū Ora	27 Sept 2019	

		breaches since 2016, have been reviewed. The analysis continues regarding: - Any other data in Tū Ora's environment and systems that the threat actors would have had access to - Access to Patient Management Systems or similar - Identify if there was the potential for lateral movement to other organisations as a result of credentials or access tokens on systems that could have been accessed			
	N/A	Provide a summary of the overall exposure risk, including the number of individual's affected and the types of information that was available.	Tū Ora	Complete.	
Validation that the new environment is secure	N/A	Tu Ora to engage with a third-party provider to conduct security assurance activities on the new website environment, and other externally facing systems, to validate that they are secure and patched.	Tū Ora	October 2019	
Legal and Privacy	N/A	s 9(2)(h) [redacted]	MOH & Tū Ora	11 Oct 2019	
Disclosure risk assessment	N/A	Detailed assessment of the risks and benefits of proactive disclosure.	MOH (with supporting agencies)	27 Sept 2019	
Communication and support to affected individuals for the Tū Ora incident					
Communications plans	Reactive comms	Create reactive communications statement in case the incident is published before Tu Ora is ready to release their planned communications post investigation.	Tū Ora (with supporting agencies)	In progress	

	Proactive comms	Create a coordinated communication plan in consultation with central agencies and Tū Ora. This will include: • Process to notify appropriate parties and individuals about the incident. • Talking points for Ministers and agencies • Q&A This work will take into consideration the potential broader system impacts.	Tū Ora (with supporting agencies)	TBD	In progress, dependent on decision regarding communication strategy and timing.
	Advice for the public	Prepare advice and FAQ's to direct people to the appropriate resources for support and advice, such as: - Netsafe - CERT NZ - NZ Police - ID Care https://www.idcare.org/ - Where to go for health support (e.g. their providers, 1737, Healthline)	Tū Ora, with support from MOH (with support from other agencies)	TBD	In progress, dependent on decision regarding communication strategy and timing.
	Contact point and agency preparedness	Confirm which contact centre(s) will handle the calls from the public. Provide them with the necessary content to handle the calls, including: - Confirmation whether their information was held by the PHO - Information on what information could have potentially been accessed - Where to go for support (e.g. CERT NZ, 1737, etc.)	Tū Ora supported by MOH	TBD	In progress, dependent on decision regarding communication strategy and timing.

		Capacity planning of Tū Ora and supporting organisations (e.g. Healthline, PHO, GP Practices, CERT NZ, and NZ Police)			
	Briefing agency CE's and Minsters	Recommend communications plan and timing to agency CE's and Ministers for approval.	MOH	TBD	
Broader health system actions					
Sector assurance activities	Ask for further assurance from the sector	Write letter to the DHB and PHO CIO's, asking for them to send us assurance that their externally facing systems are secure via letter sent 19 September, with responses due by 4 October 2019. A meeting is scheduled for 20 September to discuss this with the CIO's of these PHO's and DHB's and shared service agencies. The letter will also describe the Ministry's more active role in monitoring and improving information security in the sector and will signal our intent to do more active scans and assurance activities.	MOH	4 October 2019	
	Quick scan for critical vulnerabilities	s 9(2)(c), s 9(2)(e), s 6(a) [redacted]	NCSC	October 2019	In progress. Initial progress report expected by 11 October 2019.
	Independent third-party assessments	Create a prioritised / ordered list of organisations with rough timing estimates.	MOH	27 Sept 2019	
		Engage with panel provider(s):	MOH	4 Oct 2019	

		- Confirm budget/funding - Write a Terms of Reference for distribution to the panel member(s)			
		- Sign Statement(s) of Work - Schedule the first round of tests - Obtain written authorisations from organisations for conducting the authorised scans against their systems - Complete the independent third-party assessments for the priority organisations We anticipate the initial set of assessments will take three months to complete. Timing around remediation of the findings will depend on the technical complexity to resolve and availability of budget and resources in the organisation.	MOH	TBD	Timing depending on availability of panel providers.

Medium and longer term actions

Following is a list of further actions that will be undertaken from a medium-to-long term perspective.

Objectives / lines of effort / phases / activity	**Sub-phase**	**Tasks / Actions**	**Who is responsible for leading**	**Target timeframe**	**Comments (**including timeframes / milestones)
Stewardship response – raising the maturity of information security in the wider health sector.	Contractual guidance	Work with the GCDO and/or MBIE to provide consistent advice on contract terms & conditions around security & privacy for DHB's and PHO's contracting IT services with other providers.	MOH	Q4 2019	

	Form a health sector cyber security maturity roadmap and implementation plan	To date, the Ministry of Health has been undertaking several initiatives to improve cyber security maturity and capability throughout the health sector. These include: • s 9(2)(f)(iv) [redacted] • Forwarding relevant security vulnerability notifications to the wider health sector; • Reviewing large business cases from DHB's for security related assurance and considerations; • Providing input and advice sought by sector participants, from small GP practices all the way to large DHB's and PHO's • Recent advice on implementing Opportunistic TLS (encryption) of email services in the health sector Guidance around digital communication privacy and security Create a roadmap which may include: • Update the Health Information Security Framework (HISF) • Identify possible solutions for deployment across the sector (small + medium sized organisations) that provides protection and alerting.	MOH	Form plan by December 2019. s 9(2)(f)(iv) [redacted] Implementation beginning in Q1 2020.	

[redacted]

Ministers involved / interested:

- Rt Hon Jacinda Ardern, Prime Minister
- Hon Dr David Clark, Minister of Health
- Hon Kris Faafoi, Minister of Broadcasting, Communications and Digital Media
- Hon Chris Hipkins, Minister for State Services Commission
- Hon Andrew Little, Minister Responsible for Government Communications Security Bureau

[redacted]

Appendix B - Strategic Communications Strategy / Public Information

While planning is underway to prepared for proactive disclosure there needs to be a separate piece of work to fully understand and document the risks and benefits of proactive disclosure, so that a decision to publicly disclose or not can be made with an understanding of all the risks and consequences.

The affected PHO will lead the initial communications as they are closest to the incident, their own investigation, their remedial actions and communications with their GP practices (and patients). They will be supported by Ministry of Health, as we are leading the broader sector response and also leading efforts to improve the sector's security. Both the PHOs and Ministry are balancing the need to ensure the right information is available to those affected about increased risk (public (scam / extortion) weighted against our actions increasing the risk of further attacks (by either highlighting weaknesses or presenting a challenge of 'strengthened protections').

In light of this, there remains discussion about the level of public disclosure (number of potential records that may have been accessed) which in turn will impact on the level of public interest; and the resultant planning for managing that. The advice we have received is that public disclosure should be tempered with limitations about what we can say. That includes limitations in advice (the advice to those potentially affected is no different from the advice to everyone else); and limitations in knowledge (we are unlikely to know if anything was taken in this unauthorised access event and unlikely to know immediately about what our testing of other health agencies will show).

As we increase our monitoring and testing we are likely to find additional vulnerabilities and instances of unauthorised access. These may be in some instances reported through NZCERT's quarterly public reports but may also require a similar public facing approach to the current unauthorised access event.

Our assessment around timing of any public announcement is that we should factor in:

- the need to inform the public so they can be warned and alerted to the potential for scams and extortion
- the need to be as well informed about the present event – central agencies continue to investigate the incident and further specific advice relevant for public communications
- the need to not increase our risk of further unauthorised access – for instance to have alerted other PHOs and key health agencies so they can test and remedy any immediate related vulnerabilities
- the need to have appropriate systems and processes in place to manage public concerns – call centres; accessing information about who is affected and how; etc