MINISTRY OF HEALTH
MANATŪ HAUORA

Health Report

Update on Tū Ora Cyber Security Incident at 8 October 2019

Date due to MO:	N/A	**Action required by:**	N/A
Security level:	[redacted]	**Health Report number:**	20191935
To:	Hon Dr David Clark, Minister of Health		

Contact for telephone discussion

Name	Position	Telephone
Shayne Hunter	Deputy Director-General, Data and Digital	s 9(2)(a) [redacted]
Dr Ashley Bloomfield	Director-General of Health	s 9(2)(a) [redacted]

Action for Private Secretaries

Return the signed report to the Ministry of Health

Date dispatched to MO:

MINISTRY OF HEALTH
MANATŪ HAUORA

Update on Tū Ora Cyber Security Incident at 8 October 2019

Purpose of report

To update you on the response to the Tū Ora Compass Health cyber security incident and to seek your agreement to proactively release key information.

Key points

- The dedicated 0800 and international phone numbers are operational and fielding calls from affected individuals. Call volumes are currently manageable and we expect to progressively reduce resourcing in the contact centre in the coming days.
- The Ministry of Health is continuing to undertake security assurance work on public-facing district health board and primary health organisation systems in conjunction with the National Cyber Security Centre and independent security experts. Initial results have identified website vulnerabilities at three district health boards which have since been secured or addressed.
- Assurance work will be ongoing. The Ministry is exploring wider security issues and will shortly provide advice to you about possible actions to strengthen the system.
- There continues to be media and public interest in the cyber security incident. We therefore seek your agreement to proactively release key information about the event and our response to ensure that the public has access to all available information.

Recommendations

The Ministry recommends that you:

a) **note** that the response to the cyber security incident is proceeding as planned and the incident management response is preparing to scale down

b) **agree** to proactively release key information about our response on the Ministry's website **Yes/No**

Shayne Hunter
Deputy Director-General
Data and Digital

Hon Dr David Clark
Minister of Health
Date:

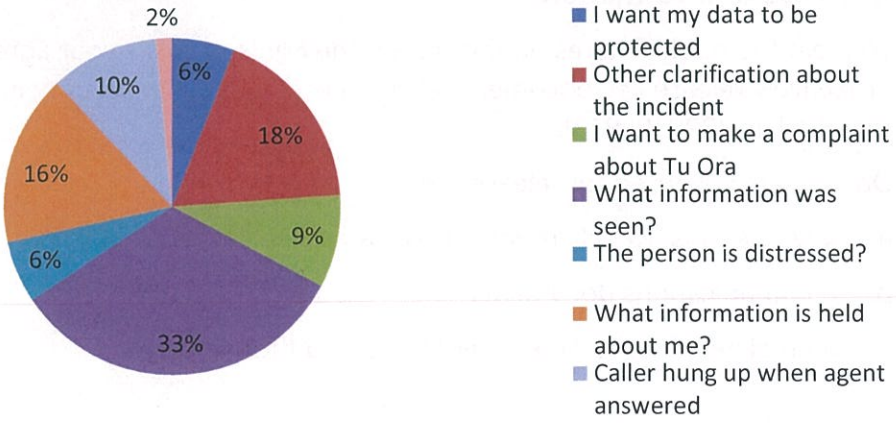
Background and context

1. Tū Ora is working closely with the Ministry of Health and the National Telehealth Service to manage issues arising from cyber security breaches discovered after the 5 August 2019 breach incident. The Ministry established an incident management team on Monday 30 September 2019 to help coordinate response efforts [HR20191913 refers].
2. District health boards and primary health organisations were briefed about the incident via teleconference on Friday 4 October 2019. Tū Ora notified general practices and practitioners later the same day.
3. Tū Ora publicly disclosed the incident on Saturday 5 October 2019. The Ministry is supporting Tū Ora to respond to media requests and public enquiries.

Our operational response is underway

Update on call centre activity

4. The Ministry established dedicated 0800 and international phone numbers staffed by customer service representatives to take calls from people affected by the incident. This was operational at 1500 on 3 October 2019.
5. Because the breach potentially affected up to one million people the Ministry established call centre capacity to cater for a significant response from affected individuals (up to 50 representatives with overflow support from the Ministry of Social Development's call centre).
6. As at 1200 on Monday 7 October 2019 the 0800 number had received 159 calls in total. Of these, 77 proceeded to a customer service representative. The remainder of callers hung up at or near the end of the recorded message. The Ministry believes that this is due to people accessing the website prompted in the recorded message.
7. A small proportion of calls handled by customer service representatives have been unable to be resolved during the call. These queries have been routed to subject matter experts in the incident management team for response.
8. The graphic below shows the types of calls received:



9. Ongoing resourcing for the 0800 will be determined by call volume and we expect to progressively reduce staffing throughout the course of this week if volumes continue to remain low. Surge staffing plans will remain in place in case of unexpected volume increases.

Update on telehealth

10. The National Telehealth Service is supporting the response by providing counselling services through 1737 and is also undertaking media and social media monitoring for Tū Ora and the Ministry.

11. As at 1300 on Monday 7 October 2019 one public call has been referred to the dedicated 1737 transfer line by call centre representatives. There have been no calls directly to 1737 that are attributed to the cyber security incident.

Communications activity is continuing

Keeping the sector informed

12. The Ministry is contacting primary health organisations outside of the affected areas to ensure that they are well briefed and able to answer any questions from members of the public. In most cases queries will be referred to the 0800 number.

13. Tū Ora is liaising with the four associated primary health organisations[1] and its wider general practice network to respond to any queries from practices and patients.

14. The Ministry will keep the sector regularly informed about developments through the business as usual communications channels (such as national health advisories) as required. No specific advisories are scheduled for the coming days.

Media and other interest

15. The Ministry is responding to ad-hoc media requests as they arise and the Director-General of Health is available for radio and tv interviews.

16. As at 1700 on Monday 7 October 2019 the Ministry had received one Official Information Act request and four written Parliamentary questions.

Proactive release of information

17. To meet the public interest in this matter the Ministry seeks your agreement to proactively release key documents about the Tū Ora cyber security incident [as signalled in HR20191913].

18. Documents proposed for release are:

    a. key briefings (weekly reports, memos and health reports)

    b. communications documents

    c. a timeline of actions taken by Tū Ora and the Ministry.

[1] Te Awakairangi Health, THINK Hauora, Cosine Primary Care Network and Ora Toa.

19. Documents will be subject to appropriate redactions in line with the principles of the Official Information Act 1982. We will liaise with your office around timing and copies of the information proposed for release will be provided to your office for review.

We are undertaking targeted security assurance actions

NCSC / GCSB assurance work

20. The GCSB's National Cyber Security Centre (NCSC) is undertaking a targeted scan of district health board and primary health organisation systems to identify a specific set of potential weaknesses, with a focus on high risk and / or potentially vulnerable areas. The full results from this scan are expected on 11 October 2019.

21. At this stage early results of this investigation identified website vulnerabilities at three district health boards. Of these, one has been secured and two have been taken offline. None of the three websites involved patient notes. The Ministry will closely monitor this situation and inform your office if further information becomes available.

Ministry assurance work

22. The Ministry has contacted all district health boards and primary health organisations to seek assurance about the security and privacy of public-facing systems by Wednesday 9 October 2019. As at 1200 on Monday 7 October 2019 we had received responses from all district health boards and 15 of 30 primary health organisations. We are stepping up engagement with any parties that have not responded or have provided insufficient responses.

23. More detailed assurance work in the form of independent external reviews of public-facing district health board and primary health organisation systems is planned. This will take some months and we will keep you and the public informed about any issues identified.

24. The Ministry is meeting with the all-of-government security panel on Tuesday 8 October 2019 to brief providers on the issue and signal the types of assurance and remediation work (if required) involved.

Next steps

25. The incident management team will continue to provide regular Situation Reports and will continue to engage with the Watch Group and ODESC. Your office will continue to receive copies of Situation Reports and any other briefing materials we prepare.

26. Resourcing for the incident management team will be scaled according to demand. We expect this to reduce over the coming days as coordination processes are bedded in and aspects of the response transition to business as usual.

27. We will report back to you with more detailed advice about the Ministry's efforts to increase its own and wider health system cyber information security, including the potential for targeted investment in due course.

ENDS.