(Binning, E. & Preston, N., 2021)

Waikato DHB cyber attack: Gr responsibility, says it has confidential patient details

By: Elizabeth Binning and Nikki Preston

25 May, 2021 02:04 PM 5 mins to read

NOW PLAYING • Waikato DHB targeted by major cyber attack

Waikato DHB's IT centre was the target of a major cyber security attack. Video / Waikato DHB ...

A group claiming to be responsible for the Waikato DHB cyber attack claims it has accessed confidential patient notes, staff details and financial information.

The district health board's entire system crashed last Tuesday during a cyber attack that has been described as "the biggest in New Zealand's history".

Some surgeries and clinics at the DHB's five hospitals have been postponed and people are being asked to stay away from emergency departments unless it is an emergency while experts try to get the system up and running again, something that is unlikely to happen this week.

The group claiming responsibility for the hack say the hijacked information includes personal ation - including financial information - of staff and patients.

5th

Waikato DHB chief executive Kevin Snee said he would not comment on the email made by the group claiming responsibility for the cyber attack because it was a matter for police.

There was a plan in place if information were made public.

Snee declined to say whether there had been any communication between the DHB and hackers, or on whether patient information had been accessed.

There was always potential that information held by the DHB could be accessed, which it had initially hoped was a "low risk" and they wanted to educate people how to respond to that if it did happen.

Snee said he would not comment on the cyber attacks because public information could influence the perpetrator.

Hack claim: 'We have a lot of personal info'

Snee yesterday acknowledged there may be some concern and anxiety about data and information held by the Waikato DHB but moved to assure patients that didn't seem to be the case.

"There is no evidence, at this point, that any data has been accessed and Waikato DHB is continuing to work with cybersecurity experts."

He did, however, urge anyone with concerns to seek ways to protect themselves and be aware of any unsolicited communications claiming to be from any government organisation.

Several hours after Snee made those comments an email was sent to some media organisations, including the Herald, claiming patients' information had been accessed.

"We stole documents and he knew it ... We have a lot of personal info of employees and patients, financial information etc," the emailer said.

"We give them 1 more chance to contact us. 1 more day."

The Herald has provided the email to police.

Police said the email is "being assessed".

The group claims to have given the DHB seven days to contact it when it launched its cyber attack but says it has not yet heard back.

It says it has deleted most of the backups but could help restore the systems if the DHB responds but that had not happened despite several attempts to contact the DHB.

"They decided to ignore us and torture their employees and patients. It is only their fault that DHB is still offline."

The GCSB's National Cyber Security Centre is providing support to the Waikato DHB.

"As we have previously stated, the NCSC knows from its involvement in other significant cyber attacks that malicious actors can monitor what is being said in the media, and this can influence their behaviour.

"For this reason we will not be providing any further comment at this time about our incident response."

The GCSB referred questions about patient information to the DHB.

Snee told reporters today that work with cybersecurity experts, the Privacy Commissioner and police on the incident response, investigation and remediation was continuing.

An 0800 number had been set up to respond to any concerns from the public around privacy of data held by Waikato DHB.

The DHB was still working towards getting some of the services back online next week.

Snee said they would be investigating why the whole system crashed and what went on: "I think it's important there's an independent review."

Snee said the DHB was working with an independent company to protect patient data.

"At the moment the system is down ... and once it gets stood up we will be taking the advice of security experts."

Health services continued to be maintained well under unusual circumstances.

Snee warned patients to be careful about unsolicited communications claiming to be from the DHB or other government organisations.

Emergency department physician Dr Gregory Stevens said staff were relying on manual processes and everything was taking much longer than it usually would.

Snee has said several government authorities were involved in investigating the cyber attack and were trying to fix the crashed system.

"We are working with the National Cyber Security Centre, GCSB (Government Communications Security Bureau) and NZ Police to undertake a full and thorough investigation to understand what has happened. The Waikato DHB has also informed the Office of the Privacy Commissioner."

Snee has said repeatedly that the DHB will not pay a ransom - a move police and cyber experts say is the best approach because paying only encourages more offending.

Ireland's public health service was this month hit by a major ransomware attack from which is it still recovering. The attackers asked for US$20 million in bitcoin but a ransom wasn't paid.