+BUSINESS | In print

Lessons learnt from PHO hack attack: Financial struggles add to challenge of cyber vigilance

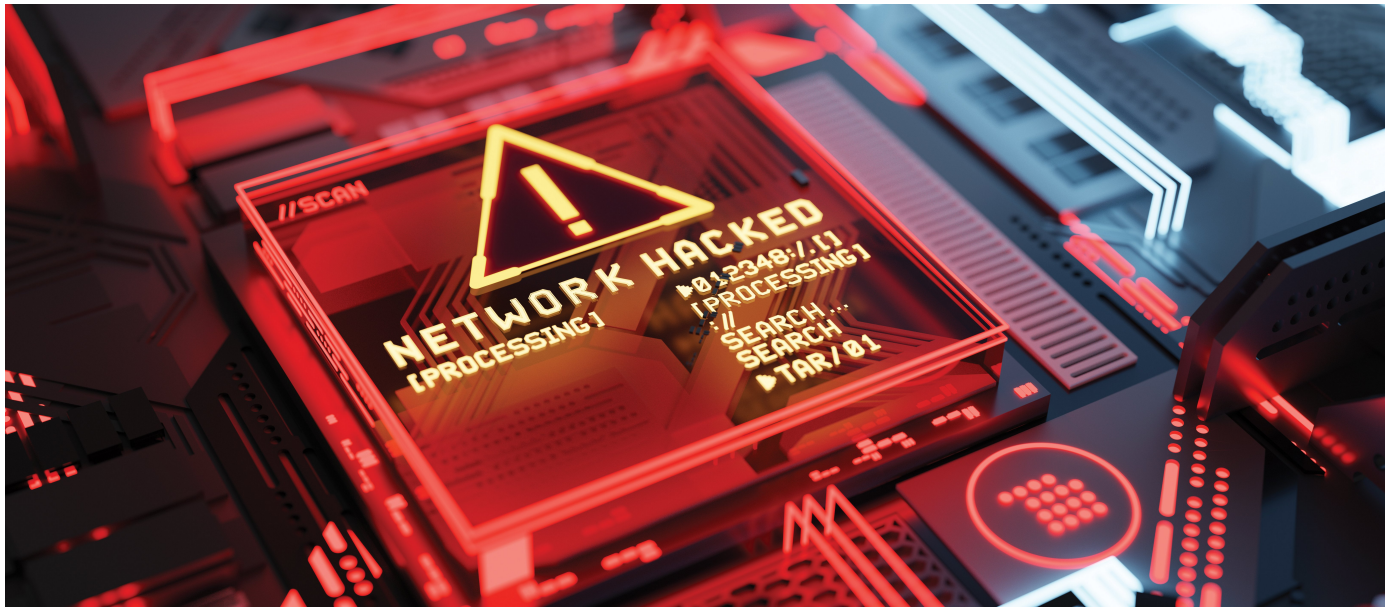
Stephen Forbes

sforbes@nzdoctor.co.nz

0

Monday 27 November 2023, 04:01 PM

3 minutes to Read



The health sector is one of the hardest-hit industries globally when it comes to cyber attacks [Image: Solarsevenon iStock]

> Pinnacle CEO Justin Butcher [Image: Supplied]

A data breach of Pinnacle Midlands Health Network last year affected hundreds of thousands of people after the PHO's system was hacked, and the attackers gained access to patient health records via a third-party server.

With cyber attacks on the rise globally, CEO Justin Butcher says safeguarding systems from vulnerabilities is a "constant battle".

Mr Butcher says improved security across the entire sector, including primary healthcare, is vital to address the threat to its networks.

"We understand firsthand the impacts a cyber attack can have on our patients and on us as an organisation. Such events can distract and divert us from our core purpose of achieving improved health outcomes for our communities," he says.

Mr Butcher says while cybersecurity requires an ongoing focus, he concedes it's tough for general practices to keep up. "When the capitation formula was implemented in 2001, with the primary care strategy and formation of the PHOs, cyber threats weren't a thing, so the funding formula has never taken into account the costs of doing business at this level."

He says with many general practices already struggling financially, more help is needed to cover expenses.

Richard Medlicott is a Wellington-based specialist GP and a long-time champion of the use of IT in health.

"We will always be a target by hackers because health data is valuable," Dr Medlicott says. "But we're custodians of our patients' data, and with that comes responsibility in terms of looking after it."

All primary practices need to be aware of the threat of cyber attacks and take steps to reduce the risks, he says. This includes the use of two-factor authentication systems, firewalls and strong passwords.

“Having an independent IT company managing your network is also really important. With a lot of cybersecurity, the vulnerability often rests with the people and not the technology.”

Dr Medlicott says something as simple as training staff to identify phishing emails can save a lot of time and money and prevent a practice from being hacked.

Unfortunately, cybersecurity is a never-ending struggle.

“The war will never be won. It’s like a series of ongoing battles,” he says.

He agreed with Mr Butcher that government funding to cover costs would help.

Global cybersecurity study

Research released by IT security company NordPass in September found cybersecurity is an issue for health systems worldwide.

The international study said health was in the top 10 industries for client data leaks. And since 2019, hackers had attacked nearly 300 health organisations worldwide.

Te Whatu Ora conducted a cybersecurity assessment of 120 primary and community healthcare providers last year. Among the respondents were PHOs, GPs, pharmacies, allied health professionals and Māori and iwi providers.

New Zealand Doctor Rata Aotearoa asked for a copy of the findings. But the agency refused to release them “due to the sensitive nature” of the report, claiming the information would have to be processed as an Official Information Act request and might be redacted.

In an emailed statement to *New Zealand Doctor*, Te Whatu Ora national chief information security officer Sonny Taite says improving IT security across the whole sector, including primary healthcare, was vital to address the threat to its networks.

A ransomware attack on the former Waikato DHB in May 2021 targeted hospital computer and phone systems to obtain information related to patients, staff and finances.

Mr Taite says Te Whatu Ora has continued working on its Cybersecurity Uplift Programme to review and improve its readiness to deal with and counter such threats.

“While the programme’s focus is on Te Whatu Ora, given the central role we play in the health system, we’re working closely with primary care and supporting them wherever we can,” Mr Taite says.

Matthew Lord is the chief information officer of PHO Tū Ora Compass Health and a member of the General Practice NZ data and digital leadership forum.

Mr Lord says thanks to the increased use of digital technology in everything from telehealth to patient portals, the threat of cyber attacks is huge.

“And that’s the challenge.

“Cybersecurity is very broad, and staying ahead of that is hard. But I think that all sectors are in the crosshairs,” Mr Lord says.

In 2019, Tū Ora Compass Health’s website was attacked as part of a global cyber incident. Mr Lord says such events have helped highlight the risks.

“We just have to keep investing and try and stay ahead of the hackers,” he says. “There’s always more you can invest in cybersecurity. But I don’t think anybody is ignoring the problem. All the PHOs have this on their radars.”

TELL US WHAT YOU THINK

Please add your comments using the comment function below and, remember, if in doubt, **check out our comment policy**.

Michelle, capture your time to Read, Watch, Listen or Delve by clicking CAPTURE.

CAPTURE

You can view your CAPTURE RECORD here.