ANU cyber attack began with email to senior staff member

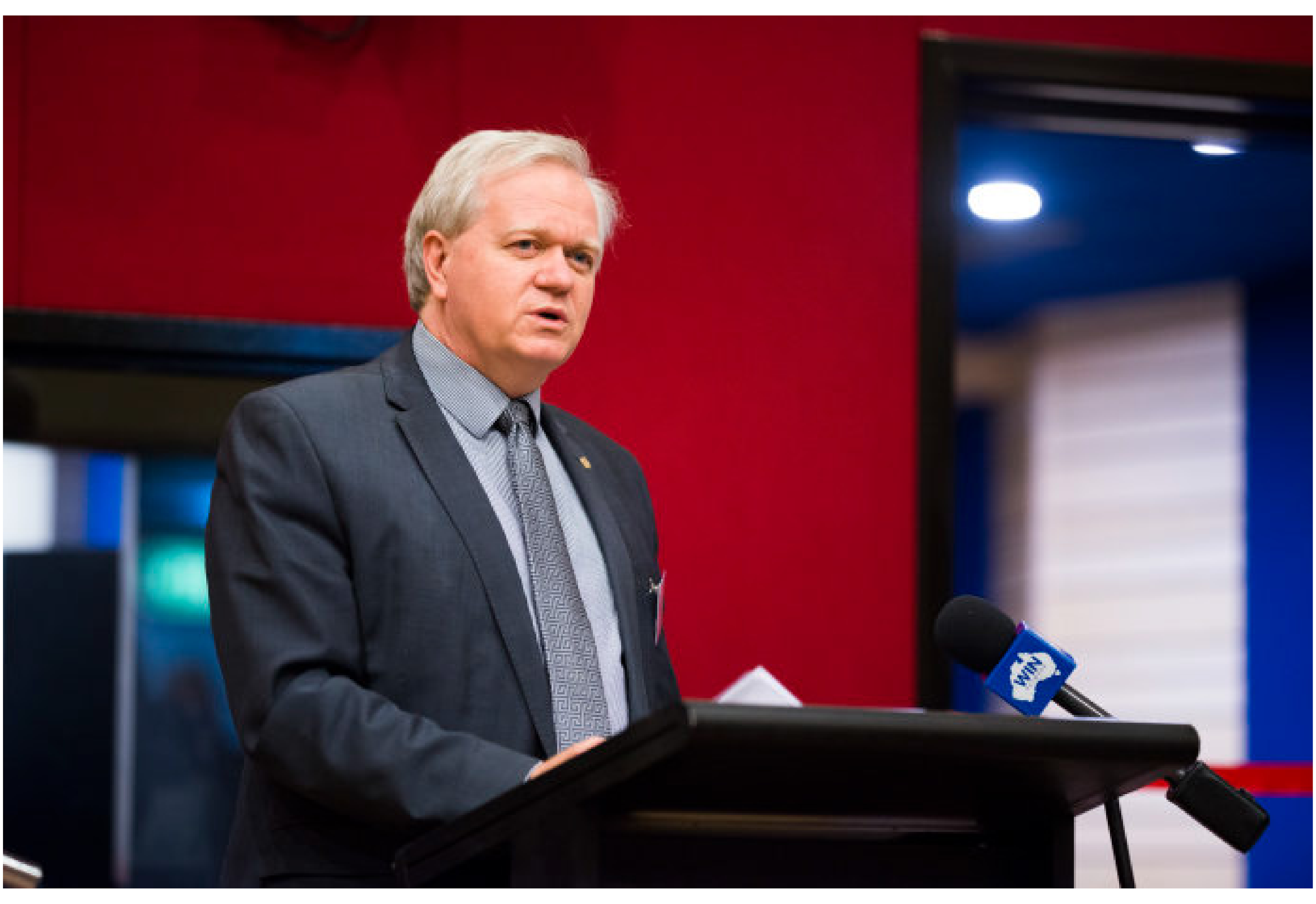
Andrew Tillett *Political Correspondent*

Oct 2, 2019 — 4.15pm

Share

The Australian National University's investigation into the hacking of students' personal data has failed to identify a culprit or exonerate suspects but the nature of the data stolen suggests fraud may have been a motive.

While some in the security community believed China was behind the cyber attack, given past form and ANU's rich trove of sensitive data and research, the university will only describe the perpetrator as a "sophisticated actor".



ANU vice-chancellor Brian Schmidt says the university needs to be transparent over a cyber hack rather than "hide in shame". **Rohan Thomson**

"It's very difficult to come up with any definitive conclusion, and speculation I think is potentially harmful," vice-chancellor Brian Schmidt said.

The hackers got away with only 700 megabytes of staff and student data – a compact disc's worth – out of the two terabytes that was stored in the compromised databases they had access to for six weeks.

The data the hackers had access to was up to 19 years old but the university cannot say which students and staff were affected or even how many.

"It's data I don't think any us would want to be shared but it's not super private," Professor Schmidt said.

Investigators estimate a team of five to 15 hackers worked round the clock and tried repeatedly to access the university's Enterprise Systems Domain, which houses human resources, financial management and student administration data.

They first successfully breached the system on November 9 last year by sending a spearphishing email to a senior member of the university's staff. While such tactics often require the recipient to click on a link or download an attachment to be compromised, the hack only required the email to be previewed for the credentials to be stolen.

Within days, the hackers were able to take control of a webserver and then a "legacy server" that was about to be decommissioned which gave access to the entire ANU network.

However, on November 30 the attackers were kicked out of the system when a new firewall was installed, but they managed to work their way back in almost a fortnight later.

ANU staff detected a fresh spearphishing attempt on December 21, which alerted them to the breach and they regained control of the system, although they thought it had been a one-off attack.

The hackers continued to try for several months after to re-enter the system.

But it was only in April when ANU's information technology staff realised the breach had been much bigger when they conducted a routine baseline threat scan.

They kept quiet for a few weeks while they investigated and cleaned up the system before going public in June.

The data the hackers had access to included names, addresses, phone numbers, birth dates, emergency contact details, tax file numbers, payroll information, bank account details and raw student academic records.

They did not have access to CVs or sensitive information such as health records, counselling or academic misconduct.

The hackers also ignored intellectual property and research data despite seeing it on the system, with investigators concluding they were just focused on the database.

While the motive is unclear, the focus on obtaining personal information is consistent with identity theft but there have been no cases of fraud emerging where this data has been misused. ANU investigators have also scoured so-called "dark web" sites for any traces of it.

Part of the difficulty in attributing blame for the attack is the hackers meticulously covered their tracks by removing traces of malware during their time in the ANU system. Investigators said this was a much more sophisticated operation than an attempted hack on ANU's systems disclosed in July last year.

"This wasn't a smash and grab. It was a diamond heist," Professor Schmidt said.

He said. the university had beefed up its cyber security and was going public to be upfront with staff, students and alumni.

"Rather than hide in shame, we need to confront the reality data was taken, we need to be transparent and we need to make sure breaches like this don't happen again in the future," he said.

Andrew Tillett writes on politics, foreign affairs, defence and security from the Canberra press gallery. *Connect with Andrew on Facebook and Twitter. Email Andrew at andrew.tillett@afr.com*