Hospital cyberattack could have been avoided

ia.acs.org.au/article/2019/hospital-cyberattack-could-have-been-avoided.html

The ransomware infection that recently crippled several Victorian hospitals could have been avoided if the planned installation of artificial intelligence-based security software had happened just a week earlier.

That software, from security vendor BlackBerry Cylance, was slated to have been installed in early October but came too late to stop the September 30 breach – in which healthcare services were interrupted after a ransomware attack shut down administrative systems in

nearly a dozen regional centres.

Security staff disconnected the systems from the Internet and scrambled to isolate the ransomware, successfully ferreting out the malware using AI techniques that learn to recognise malware based on its characteristics rather than checking against a database of known attacks.

AI has proved invaluable for Latrobe Regional Hospital (LRH), which like the other breached sites had to shut down numerous systems and was forced to transfer cancer patients to The Alfred in Melbourne for treatment.

“We have gone through and cleaned all our hardware and now we are just rebuilding services and systems and turning on other systems that weren’t impacted,” acting chief executive Don McRae said during a recent update on the health service’s recovery efforts.

“We found computers that still had the virus on it and [Cylance] shut it down very quickly.”

A state under siege

The centralisation of IT security and service delivery, which in Victoria is managed by the Department of Premier and Cabinet (DPC), means that the planned rollout would likely have been part of a Department of Health and Human Services or even a whole-of-government deployment.

A DPC spokesperson wouldn’t comment on specific security tools but confirmed that the affected hospitals – which included sites across the South West Alliance of Rural Health (SWARH) and Gippsland Health Alliance – had restored “all critical systems”.

The government “does not pay ransoms to cyber criminals”, the spokesperson said in noting the focused containment of the malware infection had seen “the best cyber minds from government and private industry unite in response”.

The response – which involved excising the malware, wiping computers and restoring from backups – was spearheaded by the Victorian Government Cyber Incident Response Service, a crack team that has handled over 600 cyberattacks on Victorian government organisations since it was established just 15 months ago.

That’s more than one attack per day – highlighting the ongoing threat to Victorian healthcare and other government agencies from a constant barrage of attacks.

In October, the Australian Cyber Security Centre (ACSC) issued a formal warning about the Emotet malware and its payload of Ryuk ransomware – the strain believed to have caused the September breaches.

Outdated technology, poor security controls, the high value of healthcare data and a broad spectrum of user habits have left healthcare organisations suffering far more breaches than any other sector.

Australian healthcare organisations reported 206 data breaches in the first year of the Notifiable Data Breach (NDB) legislation, with 90 incidents due to malicious or criminal attack.

That was in line with overseas experience: a recent review by security firm EmsiSoft, for one, identified 491 ransomware attacks on healthcare providers in the first three quarters of this year alone.

Cyber security still not an executive priority

Victoria's susceptibility to cyberattack was a core concern of a recent Victorian Auditor-General report, which tested Victorian health services' security and found that all were vulnerable to the theft or alteration of patient data.

Yet despite the state government's ongoing efforts to improve cybersecurity response, a review of health services' recent annual reports found that cybersecurity is still not an executive priority.

Newly updated Statements of Priorities 2019-2020, which are released on 1 November each year and reflect agreed priorities between Victorian public healthcare services and the Minister for Health– fail to mention cybersecurity at all.

The boilerplate statements are more concerned with clinical performance indicators and references to 'data' relate only to performance data and its submission to state authorities.

The words 'cyber' and 'privacy' do not appear at all – not even in the Statements of Priorities lodged by malware-ravaged LRH and South West Healthcare.

The word 'security' is only referenced in the context of occupational violence – issues such as physical facility protection and installation of additional lighting in staff carparks.

Similarly, a casual review of health services' annual reports confirmed that, despite years of warnings from government auditors, Victoria's health services executives remain either ignorant of cybersecurity, or see it of so little import that it doesn't merit a mention.

Given that those reports are otherwise detailed enough to even highlight improvements in the efficiency of the washing of bedsheets, cybersecurity's omission suggests that data protection still faces an uphill battle.

Healthcare isn't the only industry to struggle with this issue: a recent Thycotic-Sapio Research study found a massive disconnect between business and cybersecurity priorities that was marginalising information security executives and making them question their value to the organisation.


David Braue

David Braue is an award-winning technology journalist who has covered Australia's technology industry since 1995. A lifelong technophile, he has written and edited content for a broad range of audiences across myriad topics, with a particular focus on the intersection of technological innovation and business transformation.