Published on *The National Law Review* https://natlawreview.com

REvil STrikes Again – Ransomware Attack on UnitingCare Queensland

Article By:

Cameron Abbott

Following a ransomware infection in late April, UnitingCare Queensland has suffered a nearly 2 month long ordeal to regain control of its systems. UnitingCare was a victim of malware called Sodinokibi/REvil which encrypted its files and attempted to delete backups.

The attack shutdown a range of UnitingCare's core systems and forced its facilities to revert to paper-based and manual workarounds to continue operating.

It's been reported that the hospital and aged care facilities have now managed to bring most of its applications and systems back online. UnitingCare has confirmed that there was no evidence that any patient's health had been compromised by the cyber incident. UnitingCare is continuing to work with the Australian Cyber Security Centre and technical and forensic advisors to respond to the attack.

The private health sector has been the most heavily targeted by cyber-attacks with health accounting for 123 of the total 519 data breach notifications that were reported to the OAIC in the second half of 2020. The ACSC has reported that ransomware attacks on Australian aged care and healthcare sectors are increasing and that this increase could be due to cybercriminal's view that the healthcare sector, because of the large amount of sensitive personal medical information it holds, is a particularly lucrative target. Of course it is also a sector that is under immense stress in managing the impact of the pandemic, the last thing they need is these to be locked out of their IT systems.

National Law Review, Volume XI, Number 179