Issue - November 2021

Cyber Claims Study – Legacy System Vulnerability

Malware introduced via an unsupported system

Background to the company: The client operates six specialist medical centres in Brisbane offering dental services. They hold 50,000 personal health records, consisting of data relating to past and present clients as well as employees.

Incident: The group's outsourced IT provider noticed some unusual activity on the network, whereby there had been a lot of data moved into different files. Before he could investigate further, a message appeared on the screen – malware had been deployed into the system and a bitcoin ransom equating to $200,000 was being demanded.

Initial Response: The client followed their Incident Response Plan, which included calling the Incident Response Hotline provided to them by their Insurer. Forensic investigators immediately dove into the system to see the extent of the issue. Ransom negotiators were appointed to get in contact with the cyber criminals. They immediately noticed the language and style of the message matched a well-known ransomware distribution group, notorious for taking the ransom payment but never providing the decryption key. Forensic investigators noted the file moves but noticed that data exfiltration had not, in fact, taken place. It was found that the criminals had entered the system via a legacy system, which means that patches and updates were no longer available. A vulnerability was found and exploited, giving cyber criminals the opportunity to introduce malware.

Impact:. Incident responders recommended to the client that they restore their system and network from back-ups. They also made sure that the legacy system was taken offline and isolated from the rest of the network. The Insured lost their systems for 48 hours while the incident and restoration occurred but they deployed manual workarounds as per their Incident Response Plan to ensure they continued trading and business interruption was minimised. The incident ended up costing $73,400 in total due to forensics and system and data restoration.

Jenny Arkell
Senior Underwriter - Cyber
E: jennya@atcis.com.au
P: 03 9258 1735

Lawrence Ormrod
Senior Underwriter - Cyber
E: lawrenceo@atcis.com.au
P: 02 9928 7107

Issued by ATC Insurance Solutions Pty Ltd ("ATC") (ABN 25 121 360 978, AFS Licence No. 305802),
Level 4, 451 Little Bourke Street, Melbourne VIC 3000 acting under a binder as an agent of certain
underwriters at Lloyd's EXTF147v1