Cyber Claims Study – Ransomware Chaos Ensues at an Indoor Sports Centre

Ransomware Incident highlights the value of Incident Response Specialists

Background to the company: The client is an independent, family run indoor sports centre in a popular Sydney suburb. They employ 16 people and turnover approximately $1,500,000 annually.

Incident: One Saturday morning, the team were getting ready to open the centre. They tried to log in to the system but were completely locked out. They were unable to sign members in, look at the bookings for that day, pay invoices or do anything that required the use of their systems. They received a message from a Cyber Criminal demanding a cryptocurrency ransom in exchange for the decryption key.

Initial Response: The Insured remembered they had access to specialists to help in this situation through their Cyber Insurance, so they contacted the Incident Response Hotline for help. The Incident Responders immediately recognised the style and wording of the ransom message to be a frequently used Ransomware-as-a-Service product purchased off the dark web.

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 EXTF162v1

They were able to ascertain that the ransomware was deployed by the criminal via the Remote Desktop Protocol (RDP). The port the Insured used for RDP access was exposed to the internet, providing the hacker with a vulnerability to exploit. The cyber criminal then used email and password credentials they had purchased off the dark web, which worked to gain access to the Insured's system. The individual whose credentials were used had poor password hygiene and used the same password for multiple accounts. They also did not have Multi-Factor Authentication enabled which meant the criminal was able to gain access to the network easily.

Impact: The Incident Response specialists have access to decryption keys for known variants of ransomware and tried a few of them to regain access to the Insured's systems. Fortunately, one of them worked and after further investigation, the specialists were able to determine that no data had been compromised or exfiltrated. Thanks to the expertise of the Incident Responders, the incident was contained, and the Insured were back up and running within 2 days with the total cost of the incident being $27,400. The Insured also then enabled Multi-Factor Authentication on all remote access and implemented mandatory password changes every 3 months to prevent this kind of incident reoccurring.