Cyber Claims Study – Cyber Extortion in Action

Ransomware Incident leading to a Business Interruption and Cyber Extortion Claim

Background to the company: The client is an architectural firm with one office based in Adelaide.

Incident: A member of staff received a phishing email which contained a malicious document. When downloaded, the document released malware into the system. This prevented any access to emails, the Insured's network and files. A ransomware message appeared on all desktops demanding $75,000.

Initial Response: The Insured rang the Incident Response Hotline provided to them by their Insurer. A forensic team were appointed to deep dive into the system to find out what happened. All data files were encrypted, including blueprints and project work that would be timely and costly to recreate. Experts were appointed to negotiate with the cyber criminals about the Ransom. The message and correspondence were in line with a well-known ransomware as a service provider, known to give the decryption key when payment is received.

Impact:. The IT specialists were able to restore some files from back-ups but not all. The Insured decided to pay the ransom demand of $75,000 and receive the decryption key to fully restore the network and avoid further delays. Operations halted for 16 working days, incurring $137,600 in Reputational Harm Event and Business Interruption losses. IT specialist costs amounted to $42,841. The Insured bolstered their back-up security, including full restoration tests every 3 months to help prevent this happening again.

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 EXTF149v1