Cyber Claims Study – Manufacturer hit by Ransomware

A Ransomware Attack and Business Interruption Claim

Background to the company: The client is a manufacturer of food packaging based in New South Wales. They provide packaging to two of the biggest food production companies in Australia for both perishable and non-perishable goods.

Incident: The Insured was hit by a Ransomware attack, first discovered by the client because they could not access their systems and instead had a ransom demand message on their desktop. All 93 employees were locked out of their computers. The Operational Technology (OT) at one of the manufacturing sites was also affected, grinding production to a halt. The cyber criminals were demanding $750,000 for the decryption key.

Initial Response: The client had a Disaster Recovery Plan in place, which included ringing the Incident Response Hotline provided to them by their Insurer. After notifying the hotline, IT specialists acted quickly in an effort to lower the impact of the event. They initially looked at whether they were able to restore systems and data from back-ups and whether there had been any data exfiltration (a method used by latest ransomware strains to increase the chance of ransom payment).

Result: The result of the Ransomware attack was 4 days of operational disruption, whereby employees were unable to access systems and one plant was unable to manufacture packaging. Forensic investigations showed that the malware had originated from an employee downloading an infected attachment. There was an outbound network connection between the server and the affected plant. Luckily, the client had very good systems and data back-ups and a Disaster Recovery Plan in place. There was no evidence of data exfiltration and they did not need to pay the ransom.

Impact: The client used their other manufacturing plants to help fulfil a large order, but it was still delayed so a Public Relations Firm was hired to manage their client relations. AUD 64,827 was incurred as a business interruption claim and a further AUD 58,430 was incurred for system restoration and forensic investigation. The client ensured that segregation was in place between IT and OT networks going forward.

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 - EXTF130 v1