

Cyber Claims Study – Malicious Voicemail message

Crafty Malware Attack and Business Interruption Claim

Background to the company: The client is a tiling company specialising in commercial construction projects. They employ a team of 34 and are based in Melbourne and Adelaide.

Incident: A member of the office-based admin team received an email saying a new voicemail message had arrived. Given the phone system usually worked like this, the employee clicked on the file despite not noticing their phone ring. After opening the file, the employee's screen went blank and a ransom message appeared, saying that all their files had been encrypted and demanding \$250,000 in cryptocurrency for the decryption key. In a short space of time, all the computers were displaying the same message and emails couldn't be accessed via mobile devices.



Initial Response: The Insured started by ringing the Incident Response Hotline provided on their Cyber Policy documents. As part of their Disaster Recovery Plan, the client had saved the Incident Response Hotline number in their phone, meaning they did not need to access the system to obtain a copy of their policy documents. Ransomware negotiators were appointed to determine the type of malware that had been deployed. They advised that the Ransomware had been deployed by a group known for taking the ransom payment but not sending the decryption key. Forensic accountants determined that the email purporting to be from their voicemail provider was actually a very good imitation and that the attached file was malicious, causing malware to be deployed when it was opened.

Impact: The Insured maintained daily back-ups and were able to successfully restore 90% of the system. The final 10% was completed manually. Incident Response Costs were finalised at \$57,200. The Insured had suffered system interruption and downtime for 3 business days, incurring \$22,000 under the Business Interruption Section of coverage. PR specialists were also engaged to mitigate any reputational damage as a result of the incident.