Cyber Claims Study – Zero-Day Exploit

A vulnerability in the system leading to Unauthorised Access

Background to the company: The client is a Real Estate agent with 4 locations across Western Australia. They employ 36 people.

Incident: The firm are looking to hire more people to join their growing team and have several job advertisements on the go. The office manager received an email from a 'recruiter' with a CV attached for one of the available positions. The employee downloaded the file to open it, and only then noticed that the email address didn't look like it had come from a legitimate recruiter. The file itself would then not open, so as per the company's internal cyber security training, the employee reported it to their IT provider.

Initial Response: The Insured remembered they had nil excess under the 'Remediation Costs' section of their cyber policy, so they contacted the Incident Response Hotline for help. The forensic investigation experts identified the download as malicious and found exploit code had been deployed to the network.

This malware did not match any in their known malware database, so they concluded that it took advantage of a zero-day vulnerability. A zero-day vulnerability is a software vulnerability discovered by attackers before the vendor has become aware of it or released a patch for it, meaning they can infiltrate files and steal data.

Impact: The Incident Response specialists monitored the malware in the system and were able to use protections against similar, known malware to prevent it being used successfully. Shortly after this, a patch was released by software developers to fix the issue. Luckily, no data was compromised and the business was largely able to continue operating while the incident was occurring. Incident Response Costs were finalised at $78,210.