Australian Law Firm Hack Affected 65 Government Agencies

By Mihir Bagwe

Archived: 2026-04-05 20:16:02 UTC

Fraud Management & Cybercrime , Geo-Specific , Ransomware

Australian Federal Police, Department of Home Affairs Reportedly Among the Victims (MihirBagwe) • September 18, 2023

Image: Shutterstock

An April ransomware attack against one of Australia's largest law firms swept up the data of 65 Australian government agencies, the country's newly appointed national cybersecurity coordinator said Monday.

See Also: OnDemand | North Korea's Secret IT Army and How to Combat It

The Russian-speaking Alphv hacking group - also known as BlackCat - claimed responsibility earlier this year for hacking HWL Ebsworth, publishing in late May what it said was 1.45 gigabytes of stolen law firm data. HWL Ebsworth in June acknowledged the hack and said it had obtained a court injunction against further dissemination of confidential firm data.

In a Monday announcement, Air Marshal Darren Goldie, the first person to occupy the position of national cybersecurity coordinator, said a 16-week-long investigation had revealed that data from dozens of Australian government entities was caught up in the attack. A "large number" of private sector clients of the law firm were also affected, Goldie said.

"I stress that these agencies were clients of HWL Ebsworth and did not suffer a cyber incident themselves," he said. Speaking at a conference Monday, Goldie said the Australian federal police and the Department of Home Affairs were among the victims of the hack, The Guardian reported.

Alphv is known to target high-profile organizations that hold highly sensitive data. The Australian Cyber Security Center in April 2022 released an advisory alerting Australian organizations to be on the lookout for Alphv attacks.

HWL Ebsworth initially learned about the attack as early as April 26, through emails initially classified as spam. In one email from a sender claiming to be part of Alphv, a managing partner was urged to connect and warned not to contact authorities, according to court documents obtained by the Australian Financial Review. Alphv demanded an extortion payment of AU$4.6 million, the paper reported.

On May 8, the law firm informed the Office of the Australian Information Commissioner about the incident.
