This report will focus on the HWL Ebsworth (HWLE) data breach in April 2023, the victim HWLE is one of the largest legal partnerships in Australia which provides services to many government entities (Bernardone 2024). As this situation is still unfolding the timeline listed below is only accurate to the release of this report.

- 28th of April 2023 – HWLE discovers attack, after the threat actor (APLHV) makes an online post claiming to of exfiltrated data (HWL Ebsworth c. 2023).
- 1st of May 2023 – HWLE reports a cyber incident involving ransomware and data exfiltration (Department of Customer Service 2023).
- 8th of May 2023 – HWLE provided the initial report to the OAIC due to passing the threshold for a notifiable data breach (Department of Customer Service 2023).
- 9th of June 2023 – HWLE became aware the threat actor published 1.4TB of data (Department of Customer Service 2023).
- 15th of June 2023 – HWLE files an injunction to prevent the ALPHV and any third parties from releasing any information (Hendy 2023).
- 23rd of June 2023 – AIRMSHL Goldie is appointed as Australia's first National Cyber Security Coordinator (NCSC) in response to the breach (Borys & Al-Nashar 2023).
- 18th of September 2023 – The NCSC publicly states 65 government agencies were impacted by the breach (Department of Home Affairs 2023, p. 2)
- 20th of December 2023 – The Federal Bureau of Investigation releases a decryption tool in partnership with the Australian Federal Police (Australian Federal Police 2023).
- 15th of January 2024 – The Department of Home Affairs releases a list from October detailing 62 affected government departments and entities and the information breached (Bernardone 2024; Department of Home Affairs 2023).

Unfortunately, the exact vulnerability that was exploited has not been publicly disclosed, however, it was reported that the attackers achieved network access to a file server via an email an employee had received on their personal device (Buckingham-Jones & Pelly 2023; Mason & Pelly 2023). While the source of the information cannot be directly confirmed, a 2022 Ransomware profile on ALPHV notes that their primary access vector is through utilizing valid login credentials, either brute forced or gained in phishing attacks to access commercial RDP and VPN products (Australian Cyber Security Centre 2022, pp. 2-3). With this information, it can be inferred that the attack was potentially caused by a phishing email sent to an employee's personal email, which then provided the attacker with valid credentials to gain network access via a VPN on the employee's device. After this point there is less pertinent evidence on this specific attack, meaning the following is more speculative based on a Microsoft Threat Intelligence (2022) report which identifies the ALPHZ ransomware as being capable of a user authenticated privilege escalation via a UAC bypass, followed by encryption and data exfiltration notably the exfiltration process can take several days.

However we can utilize the profile developed by the (ACSC 2022) to understand who ALPHV are, and what their next actions may have been. To begin with ALPHV is also known as BlackCat and are Russian-speaking group that provides a ransomware-as-a-service affiliate program. Of which is a business model that allows people to pay to use the ransomware with a monthly fee model and a

percentage of profits from the attack (Baker 2023). ALPHV are believed to be tied to the groups responsible for the 2021 Colonial Pipeline ransomware attack (ACSC 2022, p. 1). And the primary initial access methods employed by the users of this software are exploiting known vulnerabilities, common security misconfigurations, and stolen credentials (ACSC 2022, p. 2).

This information is quite useful as it shows that ALPHV primarily uses known vulnerabilities and common misconfigurations. Both of which can be effectively mitigated through auditing systems for publicly known vulnerabilities and then correcting them. And then auditing configurations for issues such as default accounts, services with unnecessarily exposed ports, and lack of security hardening (OWASP 2021)

The difficult issue to address with the exploitation of valid accounts is the human element. Menachem et al. (2023) suggests multiple mitigation methods, however the easiest to apply in this situation would be restricting the use of personal devices, ensuring suitable password policies are in place with periodical changes, Account auditing based on their activity, and most importantly. User Training, without sufficient training the attack will have a high chance of reoccurring.

Additionally to improve the defense in depth, changes should be made to Remote access services. Oliveira et al. (2023) advises four primary methods to mitigate this the first is to disable remote access services, limiting remote access to sensitive information, applying Multi-factor Authentication, and network segmentation through internal firewalls and gateways so clients cannot access the full network remotely.

The breach itself is reported to of affected a majority of HWLE's clientele with approximately 4Tb of documents being leaked which has included at least 62 different government departments and agencies (Bernardone 2024; DHA 2023). Affected entities range from the Digital Health Agency responsible for the My Health Record, through to the Department of Defence. An overview was provided stating a range of PII, Medical, and National security information among many others were exfiltrated (DHA 2023, p. 4).

A notable response by HWLE was to file a legal injunction to prevent ALPHV from illegally releasing data that was illegally acquired the side effect of this however is that media companies and third party breach detection services such as HaveIBeenPwned are unable to report directly on this information (Hendy 2023). While this has helped to protect the reputation of HWLE it comes at a cost to affected individuals who have been notified they were involved in a breach but not what information had been breached (Nadel J 2024).

To conclude, this breach could have been mitigated through adequate security measures. The threat actors were known for using already reported vulnerabilities. But most critically the information of the breaches was suppressed, rightfully so with the security agencies. But at the detriment of the individuals who have had sensitive information breached from health-related agencies but have not been told what information was breached. And hopefully this situation is used as a future learning experience on how to respond to large breaches.

Reference List

ACSC – see Australian Cyber Security Centre

DHA – see Department of Home Affairs

DPSC – see Department of Customer Service

HWLE – see HWE Ebsworth

OWASP – see Open Worldwide Application Security Project

Australian Cyber Security Centre 2022, *ACSC Ransomware Profile – ALPHV (aka BlackCat)*, Australian Signals Directorate, viewed 16 January 2024, <https://www.cyber.gov.au/sites/default/files/2023-02/ACSC%20Ransomware%20Profile%20Alphv%20%2814%20April%202022%29%20-%20PDF.pdf>.

Australian Federal Police 2023, 'Russian-led hacking group disrupted as Australian businesses regain access to critical data', media release, 20 December, Australian Federal Police, viewed 16 January 2024, <https://www.afp.gov.au/news-centre/media-release/russian-led-hacking-group-disrupted-australian-businesses-regain-access>.

Baker, K 2023, *Ransomware as a Service (RaaS) Explained How It Works & Examples*, Crowdstrike, viewed 16 January 2024, <https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/>.

Bernardone, L 2024, 'RBA, AFP, AusPost caught up in law firm hack', InformationAge, 15 January, viewed 16 January 2024, <https://ia.acs.org.au/article/2024/rba--afp--auspost-caught-up-in-law-firm-hack.html>.

Borys, S & Al-Nashar, N 2023, 'Nation's first cyber security coordinator appointed, as government reckons with HWL Ebsworth breach', Australian Broadcasting Commission, 23 June, viewed 17 January 2024, <https://www.abc.net.au/news/2023-06-23/cyber-security-coordinator-appointed-ebsworth-breach/102514454>.

Buckingham-Jones, J & Pelly, M 2023, 'Revealed: Inside HWL Ebsworth's negotiations with the BlackCat hackers', The Australian Financial Review, 15 June, viewed 16 January 2024, <https://www.afr.com/companies/media-and-marketing/revealed-inside-hwl-ebsworth-s-negotiations-with-the-blackcat-hackers-20230614-p5dgf7>.

Department of Customer Service 2023, 'Cyber incident affecting HWL Ebsworth', media release, 21 June, Digital NSW, viewed 16 January 2024, <https://www.nsw.gov.au/departments-and-agencies/department-of-customer-service/media-releases/cyber-incident-affecting-hwl-ebsworth>.

Department of Home Affairs 2023, *OSE23-127 - HWL Ebsworth Cyber Breach - Government Entities Impacted*, Department of Home Affairs, viewed 20 January 2024, <https://www.aph.gov.au/api/qon/downloadestimatesquestions/EstimatesQuestion-CommitteeId6-EstimatesRoundId22-PortfolioId20-QuestionNumber127>.

Hendy, N 2023, 'Aussie law firm slaps hackers with injunction', InformationAge, 15 June, viewed 16 January 2024, <https://ia.acs.org.au/article/2023/aussie-law-firm-slaps-hackers-with-injunction-.html>.

HWL Ebsworth c. 2023, *Cyber Incident*, HWL Ebsworth, viewed 16 January 2024, <https://hwlebsworth.com.au/cyber-incident/>.

Mason, M & Pelly, M 2023, 'Hackers turn up the heat on HWL Ebsworth', The Australian Financial Review, 11 May, viewed 16 January 2024, <https://www.afr.com/companies/professional-services/hackers-turn-up-the-heat-on-hwl-ebsworth-20230510-p5d7da>.

Menachem, G, Sternstein, J, Wee, M, Somasamudram, P, Sarukkai, S, Farooqh, S & Weizman, Y 2023, *Valid Accounts, Technique T1078*, MITRE ATT&CK, viewed 16 January 2024, <https://attack.mitre.org/techniques/T1078/>.

Microsoft Threat Intelligence 2022, *The many lives of BlackCat ransomware*, Microsoft Security, viewed 16 January 2024, <https://www.microsoft.com/en-us/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/>.

Nadel J 2024, '644 NDIS users not told which medical records leaked, seven months after HWL Ebsworth hack', itnews, 19 January, viewed 20 January 2024, <https://www.itnews.com.au/news/644-ndis-users-not-told-which-medical-records-leaked-seven-months-after-hwl-ebsworth-hack-604150>.

Oliveira, A, Shuper, A, Geesaman, B, Oakley, D, Fiser, D, Tayouri, D, Frimark, I, Chen, J, Logan, M, McCune, R, Smith, T, Manral, V, Weizman, Y & Avrahami, Y 2023, *External Remote Services, Technique T1133*, MITRE ATT&CK, viewed 17 Janauary 2024, <https://attack.mitre.org/techniques/T1133/>.

Open Worldwide Application Security Project 2021, *A05:2021 – Security Misconfiguration*, Open Worldwide Application Security Project, viewed 16 January 2024, <https://owasp.org/Top10/A05_2021-Security_Misconfiguration/>.