Australian Government
National Office of Cyber Security

HWL Ebsworth Cyber Security Incident

National Office of Cyber Security | Lessons Learned Review

February 2024

Table of Contents

1 Executive Summary

On 18 September 2023, the then National Cyber Security Coordinator (the Coordinator) announced the commencement of a Lessons Learned Review into the coordination of the response to the 2023 HWL Ebsworth cyber incident (the Review). The National Office of Cyber Security (NOCS) conducted a formal lessons learned process and led the development of the Review Report (the Report). All impacted government entities who participated in the coordinated response to the incident were consulted.

On 28 April 2023, HWL Ebsworth became aware that it was subject to a cyber security incident. The incident involved the reported exfiltration of approximately four terabytes of data, which equated to approximately 2.2 million files. The data breach exposed a range of sensitive information including legal advice provided to government entities; personally Identifiable Information (PII); government information including data relating to national security and law enforcement matters; and corporate information, including client, contract, and project information.

The coordinated response to the incident was effective and supported HWL Ebsworth and impacted government entities to manage the consequences of the incident. As with the response to all cyber incidents, there are lessons that have been learned, including:

- **Central coordination and consequence management functions**, like those in the NOCS, objectively reduce the burden on impacted entities.
- **Consistent and accurate public communications** are important to developing and maintaining transparency and trust.
- Forums for **genuine government-industry engagement** in responding to a cyber security incident build trust.
- **Expectations around timely and accurate data analysis** should be managed considerately.
- Accurate and **careful management of working group membership** is integral to an effective response.
- Consideration should be given to including **broader groups of stakeholders** in the coordinated response, including both public and private sector impacted entities.
- Timely sharing of **identity credential information** to government issuing agencies can help to minimise ongoing harm to individuals.
- The **ongoing role of some regulatory agencies** in coordinated consequence management requires careful consideration.

2 Introduction

On 28 April 2023, commercial law firm HWL Ebsworth became aware that it was subject to a cyber security incident. HWL Ebsworth is the largest legal partnership in Australia and provides a range of commercial services as part of its legal and consultancy arrangements. The incident involved the reported exfiltration of approximately four terabytes of data, which equated to approximately 2.2 million files.

To date, 62 Australian Government entities have been impacted by the HWL Ebsworth cyber incident. A large number of state and territory government entities and private sector organisations were impacted by the breach.

- Australian Government entities were impacted to varying degrees in terms of the volume and nature of data exposed. As at February 2024, some Australian Government entities are continuing to work with HWL Ebsworth to manage remaining impacts as a result of the incident.
- Other impacted clients included local government entities, banks, insurers, telecommunication providers, residential property developers, non-residential property owners, construction and infrastructure clients, transport operators, as well as many other commercial entities across several sectors.

Across all impacted clients, the incident exposed a range of sensitive information, including personal information; details relating to historical and contemporary litigation matters; commercial advice; and other information relating to the operations of the law firm and its clients. This included:

- Personally Identifiable Information (PII) relating to employees or clients of government entities, including information contained in credentials and other documents, and other sensitive personal information relating to individuals.
- Government information including legal advice provided to government departments, litigation matters including migration and employment, and potentially sensitive details of projects relating to national security matters.
- Information relating to vulnerable persons, including people with a disability and the nature of their condition; victims of crime; and sensitive employment and medical information relating to specific legal matters.
- Corporate information, including employee, client, contract, and project information.

From 1 May 2023, the Cyber Security Response Coordination Unit (CSRCU) now within the NOCS supported HWL Ebsworth in a coordinated Australian Government response to manage the consequences of this incident. This coordinated response lasted for four months, and involved a significant number of bilateral meetings with HWL Ebsworth, as well as a range of multilateral meetings within government and with the firm.

Following the conclusion of coordinated support, the then National Cyber Security Coordinator determined that a lessons-learned review process be undertaken. Formal lessons-learned processes are a key mechanism under which the NOCS will support enhanced cyber security response and resilience in Australia. Lessons-learned processes enhance the understanding of government and industry on how incidents occur; where collective management of consequence works well; and where specific actions should or should not be considered in the future.

3 Scope of this Review

This **review considers the following elements** of the 2023 HWL Ebsworth cyber incident and data breach (the incident) and the coordinated response:

- The response arrangements supporting actions undertaken by and between Australian Government, state and territory government entities, and HWL Ebsworth, relating to consequences to be managed from the incident.
- Specific consequence management issues related to cyber security, legal and commercial risk, and the operation of cyber incident crisis response functions.
- How these response arrangements supported decision making and information sharing.
- Outcomes and actions underway to enhance incident response arrangements.

The review **does not** consider:

- The cause or fault relating to the incident.
- Compliance with Australian regulatory frameworks by parties to the incident.
- Any regulatory actions considered or undertaken.
- The ongoing threat posed by the threat actor, or other elements related to law enforcement.
- The initial technical incident response.

4 The coordinated response

The coordinated response to the incident included the following:

- From 1 May 2023, the CSRCU originally under Deputy Secretary Cyber and Infrastructure Security's leadership and then subsequently within the NOCS led the coordination of the Australian Government's consequence management activities. The CSRCU undertook regular and direct contact with HWL Ebsworth partners. This allowed synchronised response activity and enhanced situational awareness.
- The CSRCU coordinated three working groups to coordinate consequence management activities: the Legal Services Working Group, the Sensitive Issues Working Group, and the Identity Security and Services Working Group. These working groups involved HWL Ebsworth and relevant Australian Government, state and territory government entities. There were 29 working group meetings.
    - The Legal Services Working Group was the primary government coordination forum for impacted government clients to receive updates and engage with HWL Ebsworth. It originally focussed on legal risk to client government entities, but practically grew into a forum for situational awareness and information exchange over the life of the incident response.
    - The Sensitive Issues Working Group was convened to discuss considerations around vulnerable individuals, including notifications to persons with specific sensitivities. It also considered potential issues relevant to national security and law enforcement sensitivities in the information exposed.

  - The Identity Security and Services Working Group, which was established to respond the March 2023 Latitude Data Breach, was convened for one meeting, but was not required for this incident.

- On 3 July 2023, the National Cyber Security Coordinator (the Coordinator) assumed responsibility for the Australian Government's response to the incident. The Coordinator met with HWL Ebsworth senior leadership to discuss the Australian Government's response. The Coordinator also convened and co-chaired National Coordination Mechanism (NCM)[1] meetings on 11 July 2023 and 20 July 2023 to consider impacts on industry; and issued statements on 5 July 2023, 12 July 2023 and 21 July 2023.
- On 17 August 2023, the Coordinator determined that no further coordination for incident management activities was required.

A range of Australian Government entities supported the response to the HWL Ebsworth incident. This supported the management of specific elements of the response and the retention of operational independence where appropriate. Within the Australian Government, key agencies included:

- The Department of Home Affairs and the NOCS supported the coordination, communication and engagement across response parties in the management of consequences from the incident.
- The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) supported the initial technical incident response.
- The Australian Federal Police (AFP) supported the criminal law enforcement and investigatory elements of the incident, including coordination with state and territory law enforcement and international law enforcement partners.

A range of state and territory government entities supported the response and coordinated the response within their jurisdictions. These entities contributed to the identification and management of consequences which may have impacted their jurisdiction and others. State and territory central cyber security areas had responsibility for the coordination of flow-on engagements and briefings within their jurisdictions, including technical briefings.

5 Lessons learned process

On 15 November 2023, NOCS hosted a formal lessons learned debrief session with key Australian Government, state and territory government entities, alongside HWL Ebsworth.

Key lessons were observed across a breadth of themes:

- The benefit of a coordinated response to significant cyber security incidents.
- The operation of working groups, including membership and cadence of meetings.
- The importance of setting expectations and effective communication, particularly regarding the time required to analyse, triage and categorise large volume of data.

[1] The National Coordination Mechanism (NCM) is an Australian Government mechanism facilitated by the National Emergency Management Agency (NEMA) and is a key tool for preparing for, responding to and recovering from any crises. The NCM is a flexible tool to ensure that the full capabilities of the Australian, state and territory governments and, if required, the private sector are brought to bear during a crisis.

- The importance of government entities retaining flexibility to undertake actions to manage privacy and information security impacts arising from cyber security incidents.
- The engagement of regulatory agencies in a coordinated consequence management response.

Key insights were observed through the categories of:

- What worked well – and should be considered for future consequence management activities.
- What was challenging – and should inform a different approach to future incidents.
- Other insights – considerations for consequence management and coordination responses in other cyber response activities across government and industry.

6 What worked well?

Key lessons learned

- **Central coordination and consequence management functions** reduce the burden on impacted entities. They support a shared understanding of the incident, its progression, developments and collective actions to be taken. Consideration should be given to cadence of coordination meetings.
- **Consistent and accurate public communications** across parties responding to a cyber security incident are important aspects to developing and maintaining transparency and trust. Government and industry can work together effectively to ensure public messaging efforts are complementary.
- Forums which provide for **genuine government-industry engagement** in responding to a cyber security incident also build trust.
- Genuinely **collaborative and supportive engagement** within and between government and industry partners ensures a more sustainable response posture over the life of the incident.

Discussion

HWL Ebsworth and government stakeholders overwhelmingly noted the benefit of a centralised coordination function for significant cyber security incidents requiring consequence management. They highlighted that this reduced engagement fatigue and duplication, and supported consistency in information provided and actioned across a range of relevant stakeholders. This allowed for early identification of shared interests and challenges, and any relevant actions and solutions. This was reinforced by having government and HWL Ebsworth in the same forums, including across the purpose-built Legal Services Working Group; the Sensitive Information Working Group; and the occasions on which the National Coordination Mechanism (NCM) was convened. This developed trust in the government-industry relationship and supported greater transparency in information requested and provided.

Coordinated response efforts for data breaches often occur over a protracted period of time. Centralising and streamlining the response practically supported the capacity of response teams to manage people and processes in a sustainable manner. HWL Ebsworth noted the benefit of regular sync meetings with the CSRCU to action items raised through broader and more formal engagements. The sync meetings supported situational awareness, accuracy and allowed for an opportunity to efficiently address minor queries. Combined, this approach allowed both parties to move quickly and respond to new developments.

Working groups provided scope for thematic discussion on various aspects of the incident. Given the nature of the data impacted, stakeholders generally agreed that the number of working groups were appropriate. However, with the benefit of hindsight, HWL Ebsworth noted it would have benefited from a slightly reduced cadence of engagements throughout the analytical stage of the incident response. Overall, these meetings also ensured that participants were able to resolve issues quickly and that approaches were aligned and strengthened by the collective experience and perspective of those in attendance. Each working group allowed for greater focus on legal and commercial risk, and risk to individuals respectively, with the Sensitive Information Working Group in particular allowing for better consideration of these issues than may have otherwise occurred in individualised/siloed approaches.

Government stakeholders generally agreed that while the incident was significant, the requirement of NCMs throughout its lifecycle was unnecessary. While two separate government-facing NCMs were called to facilitate more senior-level government engagement on the response, they were ultimately not required to meaningfully support the incident. The NCMs were held during the established incident response phase, following several meetings of the Legal Services Working Group, which had already established a pattern of providing regular briefings to a significant number of government stakeholders. However, there was value in briefing senior stakeholders together for situational awareness. This reinforces the value of NCMs where broad-reaching and specific consequences at a national level are identified – such as implications for service delivery, or where a larger cohort of Australians have had significant PII exposed.

The centralised approach to public messaging ensured a harmonised approach when engaging organisations and individuals who were impacted by the incident. This included through collectively developed and shared whole-of-government talking points, media statements, and consultation on required actions and next steps. This reduced confusion and prevented miscommunication during the most significant periods of response activity and supported briefing to senior government officials.

7 What was challenging?

Key lessons learned

- **Expectations around timely data analysis** should be managed considerately. This is complicated by the pressure placed on response firms to provide timeframes which are both realistic and acceptable to all parties, and are then subject to change as the analysis progresses.
- **Careful management of working group membership** is integral to an effective response.
- Consideration should be given to including **broader groups of stakeholders** in the coordinated response, including both public and private sector impacted entities.
- Clear communication and **advanced notice of the decision to cease a coordinated government response** will ensure specific matters are addressed and the justification behind the decision understood by all parties.
- If impacted **identity credential information** is not provided to government issuing agencies in a timely manner[2], it will result in ongoing harm to individuals, and may reduce public trust in response arrangements.

[2] Timing can be impacted where Government has issued legal notice to enable receipt of this information

- The **ongoing role of regulatory agencies** in coordinated consequence management requires careful consideration, and is likely to be dependent on specific entities impacted by an incident.

Discussion

HWL Ebsworth and government entities all acknowledged the challenges in managing a large amount of exposed data, and associated issues where manual assessment and triaging is undertaken. They noted that clearer communication of evolving analysis timeframes should have occurred so that impacted entities could have considered more proactive decisions regarding their information management strategy and analysis of potential impacts.

Some government entities raised concerns with the level of visibility they had over working groups of which they were not members. The CSRCU noted the need to carefully manage the attendance of these working groups, and consider the value each organisation contributes, and their need to know specific information. It was acknowledged that broader situational awareness and the 'need-to-know' principle of information management must be supported by effective management of situational reporting. Communications designed to holistically capture the progression of an incident were most valuable when the release was well known ahead of time, for example on a daily or weekly cadence, or on a particular day.

A separate 'data and risk management' working group may have supported HWL Ebsworth and their third-party incident response provider to respond to the incident. This could have enabled them to marshal the collective expertise of relevant Australian Government, state and territory government entities. In particular, they could have received more guidance in the use of e-discovery parameters to process data.

A range of other impacted clients across industry and state and territory governments may have benefitted from inclusion in the overall coordinated response. Some government entities suggested that additional working groups or forums could have enabled a broader range of interested stakeholders to receive information, support situational awareness, and identify any issues which could be resolved collectively. However, this would have been particularly challenging in the context of the sensitivity of the impacted entity being a legal services provider, and the need to consider client privacy considerations.

The conclusion of coordinated response activities needs to be carefully managed. Following four months of coordinated consequence management, the CSRCU ceased its role in coordinating the response to the incident, while remaining available should new information come to light. Some government entities noted this occurred abruptly, and there was a clear need for earlier communication of the cessation of coordinated activities during future incidents.

Depending on the nature of the incident, engagement with some regulatory agencies might require the establishment of separate working groups or forums. These agencies needed to be kept across the policy elements of the incident, and also be included where their own information or operations may have been implicated. However, response participants suggested clarity is required around when and how regulatory agencies provide advice, or engage on a general basis, in response to an incident. These engagements are often currently undertaken on the basis of trust and good-faith agreements. While HWL Ebsworth took an active and open approach to engagement with regulatory agencies, other impacted entities may be less inclined to engage with the same level of transparency in the absence of reassurance around regulatory roles in incident response. In doing so, careful articulation and calibration will be required to involve regulators where their powers or specialities are needed to resolve an incident comparative to their investigatory and/enforcement functions.

8 What was interesting?

Key observations

- The **granting of an injunction** to HWL Ebsworth to restrict further access, publication and dissemination of the exposed data may have limited harm to impacted clients.
- **Support services are essential** for impacted individuals where very sensitive personal information is exposed.

Discussion

The granting of an injunction from the Supreme Court of New South Wales to HWL Ebsworth was a key point of interest during the management of the incident. The injunction was sought by HWL Ebsworth to restrain further access to or publication of information exposed during the incident, in an attempt to protect client data, and minimise 'online rubbernecking'. Overwhelmingly, government entities viewed this enabled better support to impacted clients (including individuals) through minimising the likelihood that other actors may access and act on the published data, and was overall viewed as a sensible step in the firm's response.

HWL Ebsworth's intention when seeking the injunction was never to stop its clients from accessing their own data, as several clients were granted exemptions to ensure access for this purpose could continue. However, the injunction also prevented accidental unauthorised access which would have been inevitable in the circumstances where clients of the firm were seeking their own information but would, in the process, further compromise the privacy of other matters unintentionally.

Support services are essential for impacted individuals where very sensitive personal information is exposed. Government entities noted that cyber incidents are seeing a range of sensitive personal information being targeted (and exploited), including medical, legal, financial, or employment information. This highlights the importance of victim support services for this kind of information exposure, including any related action required where this may interact with identity-related protection activities.

9 Applying the lessons learned

The NOCS is applying the lessons learned from the HWL Ebsworth cyber incident and data breach. As immediate next steps, the NOCS will:

1. Publish resources on the role of NOCS during a cyber security incident and how impacted organisations can request coordinated support to manage the consequences of incidents.
2. Develop a playbook for the professional services sector, which will outline how government and industry can work together to respond to an incident impacting the sector.
3. Develop processes to support broader engagement with industry and enable other directly impacted industry entities to benefit from a coordinated response to an incident.
4. Improve processes for the disclosure of relevant information relating to the coordination of incidents impacting Australian Government entities.

5. Engage with state and territory governments to better integrate their interests into coordinated consequence management activities, especially when multiple government entities within a jurisdiction are impacted by an incident.