Irrelevant

From: Libby Gregoric
Sent: l or State security info 2023 8:00 PM
To: Rachel Hunter;Filly Morgan;Kristen Foster
Cc: Jemma Baker
Subject: Re: National or State security information

OFFICIAL

Of course, Rachel.
Will organise.
Regards

Libby Gregoric
Deputy Director-General
People and Services
Department of the Premier and Cabinet
P: 07 3003 9046 M: Irrelevant
E: Libby.Gregoric@premiers.qld.gov.au

From: Rachel Hunter <rachel.hunter@premiers.qld.gov.au>
Sent: l or State security info 2023 7:29:55 PM
To: Filly Morgan <filly.morgan@premiers.qld.gov.au>; Kristen Foster <kristen.foster@premiers.qld.gov.au>; Libby Gregoric <libby.gregoric@premiers.qld.gov.au>
Cc: Jemma Baker <jemma.baker@premiers.qld.gov.au>
Subject: Re: National or State security information

OFFICIAL

Thank you all.
Can I please be briefed tomorrow morning as a priority?

Warm regards,
Rachel

Rachel Hunter
Director-General
Department of the Premier and Cabinet
Phone 07 3003 9387
Level 40, 1 William Street, Brisbane, QLD 4000

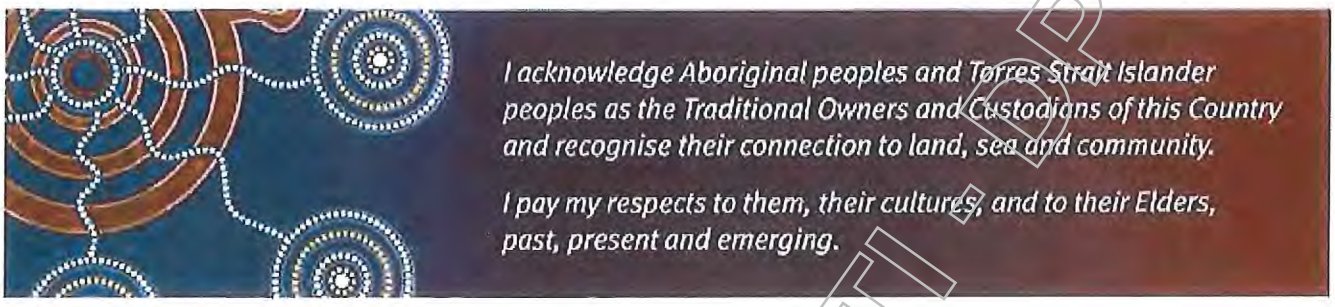
From: Filly Morgan <filly.morgan@premiers.qld.gov.au>
Sent: al or State security info 2023 6:59:36 PM
To: Kristen Foster <kristen.foster@premiers.qld.gov.au>; Libby Gregoric <libby.gregoric@premiers.qld.gov.au>
Cc: Rachel Hunter <rachel.hunter@premiers.qld.gov.au>; Jemma Baker <jemma.baker@premiers.qld.gov.au>
Subject: RE: National or State security information

OFFICIAL

Thanks Kristen.

Filly Morgan
Associate Director-General
Governance and Engagement
Department of the Premier and Cabinet
P 07 3003 9224 M Irrelevant
Level 28, 1 William Street, Brisbane QLD 4000
PO Box 15185, City East, QLD 4002

Queensland Government



From: Kristen Foster <kristen.foster@premiers.qld.gov.au>
Sent: al or State security inf 2023 6:53 PM
To: Libby Gregoric <libby.gregoric@premiers.qld.gov.au>; Filly Morgan <filly.morgan@premiers.qld.gov.au>
Subject: Fwd: National or State security information

OFFICIAL

For visibility - we will contact State securi tomorrow to address. No immediate threat known at this stage.
K

Get Outlook for iOS

From: Kristen Foster <kristen.foster@premiers.qld.gov.au>
Sent: al or State security inf 2023 6:52 pm
To: Leigh Dixon <leigh.dixon@premiers.qld.gov.au>; Harry Sukumar <harry.sukumar@premiers.qld.gov.au>; Brett Allan <Brett.Allan@premiers.qld.gov.au>
Subject: Fwd: National or State security information

Harry - Could you please contact State securit tomorrow as a matter of urgency.

Leigh - could I ask you to ask Liam to assist tomorrow with this.

Kristen

Get Outlook for iOS

From: Kristen Foster <kristen.foster@premiers.qld.gov.au>
Sent: al or State security inf 2023 6:51 pm
To: Robert Champion <robert.champion@cyber.chde.qld.gov.au>; Leigh Dixon <leigh.dixon@premiers.qld.gov.au>
Cc: Danielle Mahl <Danielle.Mahl@cyber.chde.qld.gov.au>; Christopher Polkinghorne <Christopher.Polkinghorne@citec.chde.qld.gov.au>; Andy Stokes <andy.stokes@cyber.chde.qld.gov.au>
Subject: Re: National or State security information

Thanks rob

Get Outlook for iOS

From: Robert Champion <robert.champion@cyber.chde.qld.gov.au>
Sent: hal or State security inf 2023 6:02:17 PM
To: Kristen Foster <kristen.foster@premiers.qld.gov.au>; Leigh Dixon <leigh.dixon@premiers.qld.gov.au>
Cc: Danielle Mahl <Danielle.Mahl@cyber.chde.qld.gov.au>; Christopher Polkinghorne <Christopher.Polkinghorne@citec.chde.qld.gov.au>; Andy Stokes <andy.stokes@cyber.chde.qld.gov.au>
Subject: National or State security information

Kristen / Leigh

National or State security information

CSU issued an ICT Alert on this vulnerability on the tate sec

Colleagues in State securi have shared "**Attachment A** – Media Statement" and "**Attachment B** - r State securi Cyber Incident Talking Points"

r State securit provided a technical update to State & Territory counterpart at a briefing this afternoon.
They are still working through understanding the extent of the unauthorised access and potential consequences for them.

Our telemetry tells us that National or State security information .
It is not currently known if there is any potential to impact National or State security information .
It would be prudent for you to reach out to nal or State security info to confirm any potential exposure for your networks, especially given the profile of these networks.

Further technical details are available from National or State security information
If you require any assistance please reach out to my team.

Regards,

Robert Champion
Queensland Government Chief Information Security Officer
Queensland Government Customer and Digital Group
Level 5 | 140 Creek Street | Brisbane
ph 07 3235 6918 | **m** Irrelevant | **email** robert.champion@cyber.chde.qld.gov.au

EA: Jyoti Barry – Jyoti.Barry@cyber.chde.qld.gov.au (07) 3017 5904

Thank you.

Irrelevant

From: Rebecca McGarrity
Sent: Friday, 9 June 2023 6:12 PM
To: Rachel Hunter
Cc: Michael Carey;Kyla Hayden;Michelle Wellington (DPC)
Subject: FW: HIB - HWL Ebsworth Cyber Incident (002)
Attachments: HIB - HWL Ebsworth Cyber Incident (002).DOCX

FYI.

We will reach out to the PO as well.

From: Kyla Hayden <Kyla.Hayden@premiers.qld.gov.au>
Sent: Friday, June 9, 2023 5:18 PM
To: Rebecca McGarrity <rebecca.mcgarrity@premiers.qld.gov.au>
Cc: Michelle Jackson-Hay <Michelle.Jackson-Hay@premiers.qld.gov.au>; Michelle Wellington (DPC) <michelle.wellington@premiers.qld.gov.au>
Subject: HIB - HWL Ebsworth Cyber Incident (002)

Hi there –

LPP

The brief is with you in TRIM now.

Rob Champion is briefing Min Bailey (new to this given the MOG) and DJAG are also briefing the new AG.

Did you want me to touch base directly with Darren Cann on this?

Kyla

Irrelevant

From: Fiona Toogood
Sent: Monday, 19 June 2023 2:56 PM
To: Rachel Hunter
Subject: Audit and Risk Management Committee - 20 June
Attachments: ARMC Final meeting pack - 20 June 2023.updated version.pdf

Hi Rachel

As discussed, please find attached the ARMC meeting papers for tomorrow's meeting at 9.30am.

Thank you

Fiona Toogood-Tetley
Senior Executive Officer to the Director-General
Office of the Director-General
Department of the Premier and Cabinet

P 07 3003 9387 M Irrelevant E fiona.toogood@premiers.qld.gov.au
Level 40, 1 William Street, Brisbane QLD 4000 PO Box 15185, City East, QLD 4002

Queensland Government

Department of the Premier and Cabinet and Public Service Commission
Audit and Risk Management Committee

DATE:	20 June 2023
AGENDA ITEM NO:	3.5
TITLE:	CIO Update:
PRESENTER:	Chief Information Officer (CIO)
RELATED PAPERS:	Attachment 1 – June 2023 Cyber Security Dashboard

RECOMMENDATION

It is recommended that the ARMC:

- Irrelevant
- **note** the cyber security update, including the June 2023 Cyber Security Dashboard (**Attachment 1**).

KEY ISSUES

Irrelevant

Irrelevant

Cyber planning and response planning

- The Queensland government the *Cyber security hazard plan* during May 2023. In preparation, the ITS security team has established a schedule to conduct regular test exercises of the incident response playbooks. Three exercises have been held since the last ARMC update in March 2023, with a fourth planned for June 2023.
    a. The exercises will occur every four to six weeks and will include various business representatives in scenarios that are planned against specific systems or technologies.
- Three of the four actions identified in the EY *Cyber Resilience Testing Simulation Exercise* report will be completed by 30 June 2023. This includes approval of a Data Breach Plan, Incident Response Plan, and associated playbooks.
- The fourth recommendation for establishment of an Incident Response Retainer is progressing and the scope of service will be completed by end July 2023. ITS has received advice that a new whole-of-government standing offer arrangement (SOA) for incident response retainer services will be released by end of June. ITS will review the scope of service against the SOA to determine if that arrangement will provide a more cost-effective service.

Cyber incident update

- No significant breaches or cyber incidents have been recorded as impacting DPC this quarter.
- The HWL Ebsworth legal firm breach does not impact DPC, nor does the National or State security information or State security information.
- Details of cyber security activity across DPC is contained in the Cyber Security Dashboard (**Attachment 1**).

Cyber Security Dashboard

March 2023 – May 2023
Preceding quarter

Security incident + core controls

Incidents: there have been no reportable security incidents for the period March to May 2023

National or State security information

Threat landscape snapshot

National or State security information

Significant incidents during Q2:

- National or State security information
- HWL Ebsworth data breach (no insights available)

National or State security information

ISMS Activities in progress/completed:

National or State security information

Detection and Response activities

Security operations detection and response activity in relation to vulnerabilities and threats identified with the potential to result in a significant security incident. These include responding to major vulnerability e.g. zero days and active threats to exploit (use) those vulnerabilities. Key risks prevented include data exfiltration, account takeover, website defacement.

# of major vulnerability alerts that required review for business impact 71 >	# of suspicious emails reported by staff for analysis 239 > 96	# of malicious web activity events responded to 218 > 313
# of Critical systems undergoing review of security controls efficacy 5	# advanced internet threats blocked Spyware/Adware: 4408 Malicious URLs: 1,071 Phishing sites: 1,299	# of Azure Cloud security events responded to: 6 > 15 Medium
# of jobs logged for IT Security team 267 > 242	Top inbound web-based attacks: Spyware/Adware Abuse of web apps Phishing	# of Security Events investigated 18 > 54 High

ISMS and Cyber Security Program Snapshot

The focus of the ISMS is to address non-conformances, identify opportunities to address security risks and improve the operation of the ISMS. The security program also includes a number of operational activities identified to address risks and/or gaps in the preventative and detective controls currently in place.

ISMS/Audit Activities in progress 8	Security Operations activities to address risks/gaps in controls 11	Number of systems classified PROTECTED 10
# of Major Non-Conformances addressed 2	Number of business systems in scope 103 > 107	Number of systems classified SENSITIVE 41 > 44
# of Minor Non-Conformances addressed 9	Number of systems yet to be classified 38 > 16	Number of systems classified OFFICIAL 16

DIRECTOR-GENERAL BRIEFING NOTE

Tracking Folder:	*TF/23/9811*
Document Number:	*DOC/23/136591*
Date Action Required By:	*/ /2023*

To: THE DIRECTOR-GENERAL
Date:
Subject: **HWL Ebsworth cyber incident and data breach**

Approved / Not Approved / Noted
Director-General
Irrelevant
Date: 20 / 7 /2023

RECOMMENDATION

1. It is recommended that you note:
   a) the current status of the HWL Ebsworth cyber incident and data breach (**Attachment 1**)
   b) a dedicated communications plan, including holding lines, notification approach and letter templates, has been developed by the Department of Transport and Main Roads (DTMR) in consultation with the Crisis Communication Network, affected Heads of Communications and affected Heads of Legal (**Attachment 2**).

KEY ISSUES

2. As of 6 July 2023, eight Queensland Government entities (affected entities) have been issued with interim reports from HWL Ebsworth. These entities include: Department of Eduction; Office of Industrial Relations; Queensland Health; Gold Coast Hospital and Health Service; Queensland Police Service; DTMR; Queensland Human Rights Commission; Queensland Revenue Office/Queensland Treasury.
3. HWL Ebsworth has obtained an interim injunction against the threat actor in the Supreme Court of New South Wales to assist in preventing parties from accessing or utilising data, including media outlets and third parties.
4. Some affected entities are seeking to commence making notifications to impacted parties based on harm assessments. It is noted that this may result in increased media enquires and public interest in the issue, so a statement confirming the impact of the breach on the Queensland Government will be published on the Queensland Government website.

<u>Impact Assessment Process</u>

5. Harm assessments by agencies are in progress or have been completed to assist in determining risk of serious harm and who needs to be notified, with the Office of the Queensland Information Commissioner (OIC) supporting entities.
6. LPP
7.
8. OIC Privacy Breach Management and Notifications guideline states, in general, if a data breach creates risk of harm to an individual, affected individuals should be notified.
9. Additionally, any decision regarding notification engages, and must consider, an individual's right to privacy under the HR Act. Specifically, any decision to notify or not notify an individual should not impede a right to privacy under the HR Act without due reason.
10. The Queensland Privacy Commissioner (QPC) has also provided guidance on Queensland notification requirements, with QPC's general view being that the entity with the primary relationship with the impacted party should undertake the notification.

Notification Approach

11. As harm assessments are completed by entities, they will then engage with HWL Ebsworth, DTMR (as whole-of- Government (WoG incident lead), and DJAG (as WoG incident co-lead) to confirm approaches before notification. To ensure visibility and appropriate action after notification, agencies have been asked to consult on any media queries with DTMR.
12. DTMR advise that legal and communications representatives from affected entities convened on 23 June 2023 to discuss the plan for notification, with meetings between affected Directors-General also agreeing the approach across departments must be as consistent and as timely as possible.
13. Initially, it was proposed affected agencies would send an initial letter to impacted parties with HWL Ebsworth to send out a final notification. However, HWL Ebsworth now indicates they are unsure when they will be in a position to notify and this may be weeks away.
14. Given the potential for significant delay, this approach has been determined as unsuitable for some affected entities due to the nature of the impacted information and inconsistency with the principle of preventing or limiting further harm by providing timely notification.
15. Each affected entity is advising regularly on progress of harm assessments, number of notifications anticipated per cohort (for example, commercial suppliers, staff, individuals), and whether they will be sending either an initial or detailed notification letter, and if HWL Ebsworth is going to be involved in that entity's notification process.
16. Three letter templates have been developed for individuals, suppliers/organisations and staff. While approaches may vary depending on an entity's level of risk, messaging in letters remains aligned between the approaches. These templates are included in **Attachment 2.**
17. Two statutory authorities including the University of Queensland and the University of the Sunshine Coast are also being provided support and opportunity to align with the Queensland Government approach.

Next Steps

18. At 7 July 2023, some affected agencies are ready to notify, with Queensland Health being the most advanced, and expected to commence notifications soon. While some entities are now in a position to make notifications, others are still reviewing significant volumes of documents, and some may determine not to make notifications.

19 LPP

20

21. On 5 July 2023, the Federal Government's new cyber security coordinator Air Marshal Darren Goldie confirmed a number of Federal Government entities had been impacted by the breach, 'with sensitive personal and government information released'.

22. A recommendation was put forward by the Department of the Premier and Cabinet Crisis Communication Network for DTMR to consider a WoG media release to ensure transparency in relation to the impact of the breach on the Queensland Government, including details on which individual agencies had been impacted, in line with other jurisdictions who have done so and named agencies.

23. DTMR advised their preference was not to issue a statement proactively and instead publish information on their website relating to the Queensland Government's involvement, with emphasis on the fact the Queensland Government services had not been impacted and remain secure.

CONSULTATION

24. DTMR; Reform and Delivery, Department of the Premier and Cabinet.

BACKGROUND

25. On 1 May 2023, media reported Russian-linked hacking group ALPHV/BlackCat claimed it had stolen approximately 4 terabytes (TB) of data from HWL Ebsworth, used widely across government, and then on 8 June 2023, the threat actors posted at least 1.4 TB of data.

Rebecca McGarrity
Deputy Director-General
Policy

Irrelevant

10/7/2023.

Situation Report

Law Firm HWL Ebsworth Cyber Incident and Data Breach

The information is OFFICIAL:SENSITIVE. Information may be subject to legal privilege, and no information may be shared outside of original recipients without the permission of the Queensland Government Cyber Security Unit and Department of Justice and Attorney-General.

Report Number	**9**
Date and Time	**06 July 2023, 11:00**
Authorized by	**Queensland Government Chief Information Security Officer**

Activation Status

National Cyber Security Arrangements	NCSA-5				
State Cyber Security Arrangements	QGCSA-5				
Disaster Management Arrangements	Stand down				

Key Points

- Legal and communication representatives have continued to meet to discuss the forward plan for communication to affected inidividuals and entities and to continue to undertake harm assessments.
- LPP
- Each affected entity is now confirming harm assessment progress, # of notifications anticipated per cohort (e.g. commercial suppliers, staff,

individuals etc) and which of three notification approaches is preferred based on their harm assessment outcomes:

  - Queensland government agency to provide initial notification. HWL Ebsworth to provide follow up notification.
  - Queensland government agency to provide one detailed notification – HWL Ebsworth not involved in notification process.
  - Queensland government agency to provide initial notification followed by more detailed notification.

- Three letter templates have been developed in consultation with Heads of Legal. While individual notification approaches may vary depending on an affected entities level of risk, messaging in the letters remain generally aligned between the above approaches.

Legal Considerations

-
-

LPP

Media

- General media interest surrounding this breach is increasing. Government clients (primarily at the Federal level) are being approached for comment, and news coverage is frequent.
- The Queensland Government (DTMR) has been approached once for comment by the Australian. Several other states and territories have also been approached for comment. At this time, no media on the breach has focused on or mentioned Queensland government agencies.
  - Media interest in the Queensland context is more likely as notification to affected persons or organisations by Queensland Government entities and HWLE commences.
- An updated WoG communications pack has been prepared that reflect the revised situation and notification approaches. It will be circulated to affected entities once DG DTMR approved.

- The Australian has again run an article today, 6 June 2023, discussing the cyber breach and impacts on Australian Government Departments.
- To ensure visibility and appropriate action, Queensland Government entities have been asked to forward any media queries to DTMR Strategic Communications Unit to coordinate.

Response Coordination

- This is a national incident being centrally led by the Department of Home Affairs. DTMR and DJAG continue to participate in the National Legal Services Working Group to inform WoQG consequence management and work to minimise any potential harm.
- Consequence management actions in response to the breach are focussing on any information confirmed as stolen and identified as sensitive or personally identifiable. Focus will then shift onto actions and considerations for the management of commercial information.
- The incident management team for this event are also meeting and communicating as required to inform the WoG response. The team is comprised of:
    - DTMR QGCSU, (lead): Strategic Communications Unit
    - DJAG (co-lead): Legal Services Coordination Unit
    - DPC: Law and Justice Policy, Crisis Communication Network
    - Affected agencies: Heads of Legal, Communication, and Digital
- The QGCSU are closely monitoring media and will circulate updated situation reports and content as the situation develops or on receipt of updated advice to governments.

Notification Process

- After completing harm assessments, all **8** affected entities will be working with HWLE, DTMR, and DJAG to commence notifing impacted individuals, organisations, or staff using WoG approved templates provided by DTMR. The following table provides a summary of the template to be used depending on the cohort impacted.
    - Statutory authorities (**2** - University of Queensland and University of the Sunshine Coast) are being provided support, and the opportunity to align with the WoG approach.
- Where an affected entity identifies any requirement to make a large number of notifications, the QGCSU and DJAG will work with that entity to determine if additional communications support is required to help manage any potential follow on queries.

Cohort	Template Title	Signature Authority	Recommended usage	Notifications to QGCSU/DJAG
Individuals	1 – Qld Government to Individuals	Agency Chief Executive or appropriately senior delegate	Affected entity completes harm assessment and determines where there is a legal obligation to notify affected individuals. Complete template and send to any/all impacted individuals. Note: even where there is no legal requirement, agencies may opt to notify affected individuals. Human Rights impact assessment to be carried out.	All summary of all notifications made by entities to to impacted cohorts must also be sent to: - Irrelevant - While the QGCSU/DJAG do not need individual copies of the notifications, the summary should include the following for WoQG centralised visibility and tracking: - # of notifications per cohort - Names of affected persons/organisations in each cohort
Organisations/third parties	2 – Qld Government to Organisation / Third Party	Contract manager or appropriately senior delegate	Affected entity completes harm assessment and determines where they would like to notify affected organisations/third parties of the breach for transparency and awareness (no legal compliance	

			obligation). Complete template and send to impacted organisations/third parties.	
Staff	2 – Qld Government to Staff	Contract manager, Divisional Head, appropriately senior delegate	Affected entity completes harm assessment and determines where they would like to notify staff of the breach for transparency and awareness (no legal compliance obligation). Complete template and send to impacted staff.	

LPP

Court Injunction

- HWLE obtained an interim injunction against the threat actor group ALPHV (Blackcat) in an ex parte hearing in the Supreme Court of NSW.
- HWLE anticipates that the injunction (and the principles of contempt of court) will assist to prevent other parties who are on notice of the orders from accessing or utilising the data, including media outlets or any other third parties who see fit to go and access the data.
- The Injuction was extended, with slight variations, until further order, with the matter stood over to 18 July 2023.
- HWLE is mindful of legitimate purposes for which clients may need to have access to their information that is published on the dark web. The goal of the injunction is to protect as best as possible the confidentiality of that data for the benefit of all clients.
- In seeking to restrain the activities of the threat actor or other parties with no legitimate interest in the data, it is not HWLE's intention to stop clients having access to data that is theirs.
- That is why the orders include a consent provision to enable such consent to be given to clients or genuinely interested parties. HWLE have asked the court to specifically note that the firm intends to engage with affected third parties to determine if such a consent regime for access can be agreed.

Background

- On **1 May 2023**, One of Australia's largest legal partnerships, HWLE, reported a cyber incident.
- HWLE operates across Australia, servicing a significant number of government and commercial clients. It has over 269 partners, with its head office in Melbourne.
- HWLE primarily provides legal services in the areas of building and construction, general corporate and commercial, taxation and revenue, technology and intellectual property, workplace health and safety, general litigation and resourcing (i.e., secondees).
- The incident involved ransomware, and Russian linked hacking group ALPHV (Blackcat) claimed to have exfiltrated approximately **4TB of data** and were threatening publication of that data to the darkweb.
- On **8 May 2023**, HWLE provided initial notification to the Office of the Australian Information Commissioner under the Notifiable Data Breaches scheme.
- As a nationally significant cyber incident, the Australian Government Department of Home Affairs have been leading the response to the cyber incident and breach in partnership with governments and HWLE since 1 May.

- The Queensland Government Cyber Security Unit (QGCSU) within the Department of Transport and Main Roads(TMR) and the Department of Justice and Attorney-General (DJAG) have led representation and response activity for Queensland.
- As part of the nationally led response, all states and territories undertook work to understand their potential level of exposure and the associated levels of risk immediately after receiving advice of the breach.
- In terms of volume of engagement, TMR and DJAG worked with agencies to identify over 2,000 matters across the last 4 financial year periods starting from 2019-20. Primary engagement occurs through Whole of Government legal and professional services panels.
- Concern for potential exposure arising from these engagements was primarily related to personally identifiable information with varying levels of sensitivity. Some potential higher risk cohorts were also identified.
- HWLE publicly committed to not paying a ransom in an effort to prevent the unlawful publication of data.
- On **9 June 2023** the threat actor unlawfully published at least 1.4TB of HWLE's data on their leak-site after threatening to do so.
- The TMR notified the Australian Cyber Security Centre (ACSC) of the post immediately, and convened a response team to manage the WOQG response alongside the Department of Home Affairs as National lead.
- Online media began appearing shortly after. This breach has attracted significant media scrutiny to date and is likely to continue to do so, with coverage-to-date in all the major press.
- Unfortunately, the bulk of data analysis to understand what had been stolen and which government agencies had been impacted had not yet been finalised by HWLE before this data dump occurred.
- States and territories were not authorised to download data for the purposes of matching and/or assessment (to understand the data affected and impact) To do so without authorisation would likely constitute an interference with privacy under s13 of the *Privacy Act 1988* (Cth).
- As a result, states and territories were not aware of what data had been taken, which agencies had been impacted, and proactive notification and consequence management could not occur.
- Since the first leak, HWLE have been working to urgently expedite data analysis and issue affected government agencies with interim reports and documents to enable concurrent harm assessment.

1

The information is OFFICIAL:SENSITIVE. Information may be subject to legal privilege, and no information may be shared outside of original recipients without the permission of the Queensland Government Cyber Security Unit and Department of Justice and Attorney-General.

2

2

Contents

- Introduction
- Background
- Update
- Comms Plan
- Media Approach
- Q and A's
- Other useful information

Department of Transport and Main Roads

3

Introduction

- On **1 May 2023**, One of Australia's largest legal partnerships HWL Ebsworth (HWLE) reported a cyber incident.
- HWLE operates across Australia, servicing a significant number of government and commercial clients. It has over 269 partners, with its head office in Melbourne.
- HWLE primarily provides legal services in the areas of building and construction, general corporate and commercial, taxation and revenue, technology and intellectual property, workplace health and safety, general litigation and resourcing (i.e., secondees).
- The incident involved ransomware, and Russian linked hacking group ALPHV (Blackcat) claimed to have exfiltrated approximately 4TB of data and were threatening publication of that data to the darkweb.
- On **8 May 2023**, HWLE provided initial notification to the Office of the Australian Information Commissioner under the Notifiable Data Breaches scheme.
- On **9 June 2023** HWLE became aware that the threat actor had published at least **1.4TB** of exfiltrated data on a dark web breach site.

HWL EBSWORTH
LAWYERS

Department of Transport and Main Roads

4

4

Background

- As a nationally significant cyber incident, the Australian Government Department of Home Affairs have been leading the response to the cyber incident and breach in partnership with governments and HWLE since 1 May.
- The Queensland Government Cyber Security Unit (QGCSU) and the Department of Justice and Attorney-General (DJAG) have led representation and response activity for Queensland.
- As part of the nationally led response, all states and territories undertook work to understand their potential level of exposure and the associated levels of risk immediately after receiving advice of the breach.
- In terms of volume of engagement, the QGCSU and DJAG worked with agencies to identify over 2,000 matters across the last 4 financial year periods starting from 2019-20. Primary engagement occurs through Whole of Government legal and professional services panels.
- Concern for potential exposure arising from these engagements was primarily related to personally identifiable information with varying levels of sensitivity. Some potential higher risk cohorts were also identified.
- HWLE publicly committed to not paying a ransom in an effort to prevent the unlawful publication of data.
- On 8 June 2023 the threat actor unlawfully published at least 1.4TB of HWLE's data on their leak-site after threatening to do so.
- The QGCSU notified the Australian Cyber Security Centre (ACSC) of the post immediately, and convened a response team to manage the WOOG response alongside the Department of Home Affairs as National lead.
- Online media began appearing shortly after. This breach has attracted significant media scrutiny to date and is likely to continue to do so, with coverage-to-date in all the major press.
- Unfortunately, the bulk of data analysis to understand what had been stolen and which government agencies had been impacted had not yet been finalised by HWLE before this data dump occurred.
- States and territories were not authorised to download data for the purposes of matching and/or assessment (to understand the data affected and impact) To do so without authorisation would likely constitute an interference with privacy under s13 of the *Privacy Act 1988* (Cth).
- As a result, states and territories were not aware of what data had been taken, which agencies had been impacted, and proactive notification and consequence management could not occur.
- Since the first leak, HWLE have been working to urgently expedite data analysis and issue affected government agencies with interim reports and documents to enable concurrent harm assessment.

5

5

Update - where are we now?

- HWLE have issued ten Queensland Government entities with interim reports that encompassing over 40 matters and 5,000 documents in total:
  - Education Queensland
    - Office of Industrial Relations
  - Queensland Health
    - Gold Coast Hospital and Health Service
  - Queensland Police Service
  - Department of Transport and Main Roads
  - Queensland Human Rights Commission
  - Queensland Revenue Office
  - University of Queensland
  - University of the Sunshine Coast
- The reports reflect the progress made to date on the analysis of all documents that HWLE believe have been accessed by the threat actor. They also indicate if the material was unlawfully published.
- Data analysis processes are approximately 90 per cent complete, and updated and/or new reports will be issued to affected parties as that process is finalised over the coming week or so.
- All bar one of the above entities have received access to the documents identified as impacted in reports issued. Assessments are now being completed by each entity to understand the likelihood for serious harm, and to determine who needs to be notified about the breach.
- The Office of the Queensland Information Commissioner (OIC) has provided guidance material and tools for affected entities to assess the risk of serious harm, and determine who needs to be notified.
- Legal and communications representatives have continued to convene from 23 June to discuss the forward plan for notification.
- Meetings between applicable leads in affected departments has seen general agreement that the approach across entities be as consistent as possible and timely (limiting potential for harm where identified).
- Initially, it was proposed that agencies send out an initial letter to affected parties with HWLE to send out a final notification letter. HWLE has now indicated that they do not know when they will be in a position to send out notification letters.
- Given the potential for significant delays, some agencies are unable to utilise this approach given the nature of their impacted information and inconsistency with the principle of managing harm by providing timely notification.
- Each entity is now confirming harm assessment progress, # of notifications anticipated (per cohort – e.g. commercial suppliers, staff etc) and which of notification option is preferred based on harm assessment outcomes:
  - Queensland government agency to provide initial notification. HWL Ebsworth to provide final notification.
  - Queensland government agency to provide one detailed notification – HWL Ebsworth not involved in notification process.
  - Queensland government agency to provide initial notification followed by more detailed notification.
- Messaging and templates remain consistent and aligned between the above approaches. After harm assessments are completed, individual approaches will be confirmed with HWLE, QGCSU and DJAG before notification commences.

6

6

Comms Plan

7

7

The approach

- DTMR is lead agency for the WOQG response to this event.
- The incident management team for this event is convening as required. This group is comprised of the QGCSU & DTMR Strategic Communications Unit (lead), DJAG (co-lead), Department of Premier and Cabinet, and affected entity heads of legal and communication contacts.
- Broader Heads of Communication and Legal are being updated on a regular basis as the situation develops, and are discussing the situation as required.
- To ensure visibility and appropriate action, all Queensland Government entities have been asked to consult on any media queries with DTMR prior to response.
- The QGCSU is working with DJAG to issue any agreed guidance/instruction for Queensland Government entities in alignment with national approaches, Crown Law advice or OIC guidance.
- The QGCSU is circulating situation reporting on receipt of updated advice to governments. Eight situation reports have been issued to date on the HWLE cyber incident and data breach.

TMR Contacts

Nic Davis
Executive Director – Strategic Communication
Irrelevant
Nicole.z.davis@tmr.qld.gov.au

James Murphy
Director – External Affairs
Irrelevant
James.x.murphy@tmr.qld.gov.au

Danielle Mahl
Manager – Incident Response and Communications
Queensland Government Cyber Security Unit
Irrelevant
danielle.mahl@cyber.chde.qld.gov.au

8

8

The approach

1

Identify who has been affected

- As part of the Nationally led response, HWLE have been conducting data analysis and issuing reports to identify which government entities have been affected by the breach.

2

Provide list of affected files to government agencies

- If impacted, lists of impacted matters and access to the documents are being provided by HWLE to Qld government agencies.
- Agencies are conducting harm assessments to identify notification and disclosure requirements.

3

Government agencies send letter to affected staff/clients/ suppliers/stakeholders

- Each government agency to utilise the notification approach and template/s suitable to circumstance and send correspondence to each person/agency/supplier/ staff member/organisation.
- If a staff member is affected, the agency also identifies internal support contact.
- Agencies also to provide Employee assist numbers to staff.
- Broader stakeholder group to be identified if appropriate and required for example, unions if staff affected.
- HWLE advised of approach prior to mail out.

Note: draft correspondence appendix A

4

HWLE will then follow any interim correspondence or actions up with parties as required and work directly with them from that point onwards.

Department of Transport and Main Roads

9

9

Communication Tactical plan

Item	Publish date	Activity	Description	Audience	Cost	Responsible Area	Status
1	26 June	Communication Plan Drafted	• Draft plan circulated to relevant agencies	Heads of Communication (HOC)	Nil	• TMR Strategic Comms	Drafted
2	26 June	Holding Statement and Q and A's	• Holding Statement and Q and A's shared as part of Comms plan	HOC and Heads of Legal (HOL)	Nil	• TMR Strategic Comms	Drafted
3	26 June	Draft Letter	• Draft letter circulated to agencies	HOC and HOL	Nil	• TMR Strategic Comms	Drafted
4	27 June 04 July	Feedback from agencies	• Feedback received from agencies #1 • Feedback received from agencies #2	HOC and HOL HOC and HOL	Nil	• TMR Strategic Comms	Drafted
5	05 July	Finals approved and circulated	• Finals circulated to agencies	HOC	Nil	• TMR Strategic Comms	
6	From 05 July	Weekly meetings established	• TMR to facilitate 15 min check in on Mondays	Key agencies	Nil	• TMR Strategic Comms	

June 2023

10

10

Media

11

11

Media update

General media interest surrounding this breach is intensifying. Government clients (primarily at the Federal level) are being approached for comment.

The Queensland Government (DTMR as lead) has been approached once for comment by the Australian.

Several other states and territories have also been approached for comment.

At this time, no media on the breach has focused on or mentioned the Queensland Government as a whole or specific Queensland Government entities.

Media interest in the Queensland context is more likely as notification to affected persons or organisations by Queensland Government entities and HWLE commences.

To ensure visibility and appropriate action, Queensland Government entities have been asked to consult on any media queries with DTMR Strategic Communications Unit prior to response.

Department of Transport and Main Roads

12

Media – Holding Statement - QLD Gov (high level)

The Queensland Government is aware of a cyber incident and data breach impacting law firm HWL Ebsworth.

The Queensland Government is working with HWL Ebsworth and relevant Commonwealth agencies as the extent of the breach is investigated, including impacts to government information.

This includes work to understand and manage potential consequences of the theft and publication of the data, and to ensure that all notifications are made to affected parties where required.

Specific enquiries relating to this incident should be directed to HWL Ebsworth.

Department of Transport and Main Roads

13

Media – Holding Statement - QLD Gov (more detailed)

On 8 May 2023, HWL Ebsworth reported a data breach to the Office of the Australian Information Commissioner (OAIC) under the Notifiable Data Breaches (NDB) scheme.

On [[date]], HWL Ebsworth advised the [[Departmental/agency/as appropriate]] that documents relating to a limited number of [[Departmental/agency/as appropriate]] files were included in the breach experienced by HWL Ebsworth.

The Department of Home Affairs continues to work with HWL Ebsworth and affected Government agencies as it investigates the extent of the breach, including exposure of Queensland Government information and related consequences arising from this exposure.

[[Departmental/agency/as appropriate]] takes the privacy of its data holdings seriously and is working with HWL Ebsworth to understand what information may have been disclosed.

Should our clients' personal information be affected, the [[Departmental/agency/as appropriate]] will work with HWL Ebsworth to ensure affected individuals are notified as soon as possible, and offer assistance and support as required.

The [[Departmental/agency/as appropriate]] is committed to ensuring appropriate systems are in place to maintain the privacy and the protection of personal information.

The [[Departmental/agency/as appropriate]] systems have not been compromised.

Department of Transport and Main Roads

14

14

15

Q and A

Question	Answers
How long until individuals impacted by the breach will know?	• We understand HWL Ebsworth has begun making notifications to the OAIC under the notifiable data breaches scheme, and to some impacted entities and individuals. • The Queensland Government is working with HWL Ebsworth as part of a national response to ensure affected parties are notified as soon as possible.
How are government disrupting any unlawful access or distribution of stolen data?	• HWL Ebsworth has been granted an injunction by the Supreme Court of NSW regarding the information that threat actor claimed to have published, seeking to restrain the activities of the threat actor, and prevent additional access by other parties. The Queensland Government strongly discourage people from accessing stolen sensitive or personal information from the dark web. We should not feed into the business model of cyber criminals. • Law enforcement will take swift action against anyone attempting to benefit, exploit or commit criminal offences using stolen data. Downloading or assessing stolen data may constitute a criminal offence.
Is Government data affected? - Affected Queensland Government entities & notification timing	• Where notified, Government agencies are working with HWL Ebsworth to understand and manage the consequences of the theft and publication of the data, and to ensure that all notifications are made to affected parties where required. • Affected agencies will work to their own timeframes to fulfil notification obligations, depending on when they receive all the necessary information to complete an assessment of the data affected. • This means that not all agencies will be in a position to report on their exposure to the OAIC and affected individuals at the same time.

Department of Transport and Main Roads

16

16

Q and A

Question	Answers
Is Government data affected? - Queensland Government entities who have not received a notification.	• The Queensland Government continues to work with HWL Ebsworth to understand the extent of information exposed by the breach. ◦ This process is ongoing. • HWL Ebsworth is yet to advise **[Dept/Agency/Entity]** of any impacts to agency data arising from the breach.
Is Government data affected? - Queensland Government entities who have received a notification and are preparing to notify	• We have been advised by HWL Ebsworth that some agency data has been exposed as part of the cyber incident. • We are working with HWL Ebsworth to understand what data has been compromised and will work to notify affected parties of the breach.
Is Government data affected? - Queensland Government entities who have received a notification and have commenced notifications	• We have been advised by HWL Ebsworth that some agency data has been exposed as part of the cyber incident. • We have begun notifying affected individuals.

Department of Transport and Main Roads

17

17

Q and A

Question	Answers
What are government doing in response?	• The Department of Home Affairs is leading the coordination effort in response to the potential harm that may be realised from this incident. • HWL Ebsworth is continuing to undertake investigations, and the Queensland Government is working with multiple agencies as part of the national response effort to provide support, assess potential consequences, and minimize any harm that may arise. • The Australian Signals Directorate's, Australian Cyber Security Centre (ACSC) is engaging with HWL Ebsworth and is offering cyber security technical advice and assistance. • The ACSC leads the Australian Government's efforts to improve cyber security, including providing timely advice to individuals and businesses.
What will happen if Government data is affected?	• The Queensland Government is involved in the Nationally led coordination effort in response to consequences of this incident. This will help ensure that impacted victims receive appropriate support. • Two working groups have been established to address specific issues relating to sensitive information, & legal services. These working groups are meeting to assess potential consequences resulting from information which may be exposed as a result of the incident. • A Sensitive Information Working Group has been established to discuss the management of any information exposed related to vulnerable people, national security, and law enforcement matters. • The Legal Services Sector working group, led by the Department of Home Affairs, is continuing to meet and discuss the potential impact on the Government as a user of HWL Ebsworth's legal services. This working group is made up of legal services representatives from impacted jurisdictions and is supporting consequence coordination functions.

Department of Transport and Main Roads

18

18

Q and A

Question	Answers

As an individual what do I need to do to reduce my risk?	• While it is unclear what data may have been accessed, individuals should always take steps to protect their information and avoid any potential scams:
	• Individuals should be alert for scams referencing the HWL Ebsworth data breach. Those affected can learn how to protect themselves from scams by visiting the Australian Competition and Consumer Commission's (ACCC) ScamWatch site, www.scamwatch.gov.au, and refer to the data breach fact sheet - https://www.accc.gov.au/publications/protect-yourself-from-scams-after-a-data-breach-fact-sheet
	• For individuals who are concerned that their information may have been compromised as part of this breach, simple steps to boost cyber security include:
	  • Update your device and turn on automatic updates to ensure you always have the most up-to-date security protection.
	  • Turn on multi-factor identification to increase the security of your accounts and make it harder for criminals to gain initial access to your device.
	  • Turn on automatic backups to copy and store critical information.
	  • Implement access controls to limit user access to only what is needed on devices.
	  • Turn on ransomware protection measures.
	  • Prepare a Cyber Emergency Checklist to reduce stress and recovery time.
	  • Stay up to date on cyber security threats and trends with ACSC Alert Service.
	  • Visit cyber.gov.au for more information.
	• The Office of the Australian Information Commissioner (OAIC) has also published advice for individuals on how to reduce risks of harm following a data breach.

Can we trust / accept emails from HWL Ebsworth?	• HWL Ebsworth have provided final third party assurance that their systems are secure and there has been no further unauthorised activity detected.

19

Other helpful information

20

Notification considerations and Obligations

- Depending on the outcomes of document review and harm assessment Queensland entities may be subject to notification obligations under the Privacy Act 1988 (Cth), the Commonwealth Notifiable Data Breaches Scheme, and the Human Rights Act 2019 (Qld).
- In the Queensland context, the *Information Privacy Act 2009* does not contain any positive obligations on a Queensland agency, or its service provider, to give notifications in the event of a privacy breach.
- The Queensland Office of the Information Commissioner's Privacy Breach Management and Notifications Guideline states that, in general, if a data breach creates a risk of harm to an individual, the affected individuals should be notified.
- Additionally, any decision regarding notification engages and must consider an individuals right to privacy under the *Human Rights Act 2019*. Specifically, any decision to notify or not notify an individual should not impede a persons right to privacy under the act without due reason.
- LPP
- The QGCSU and Legal Services Coordination Unit in DJAG met with the Queensland Privacy Commissioner (QPC) on Thursday 15 June 2023 to provide a briefing and seek guidance on Queensland notification requirements for affected agencies.
- The QPC recommended that affected agencies prioritise an assessment of the matters/documents that are more likely to result in greater harm over those which don't, on face value, appear to be as serious.
- The QPC also encouraged agencies to be proactive with their investigations, so when notified of/or provided with what documents have been breached they will be in a position to respond quickly.
- The general view of the QPC is that the entity with the primary relationship with the impacted person/organisation should undertake the notification. Advice from the QPC on notification and reporting has been circulated to affected agencies.
- LPP
- LPP

21

21

Draft letters to affected individuals and parties

Note: Effected agency legal heads and executives may be required to adapt draft WoG communications to suit individual circumstances.

The high level tone and feel of the communications will remain the same.

Where adaptations are not significant, this will occur without the need for additional DTMR or DJAG approval.

22

22

Notification Approach Summary

Cohort	Template Title	Signature Authority	Recommended usage	Notifications to QGCSU/DJAG
Individuals	1 – Qld Government to Individuals	Agency Chief Executive or appropriately senior delegate	Affected entity completes harm assessment and determines where there is a legal obligation to notify affected individuals. Complete template and send to any/all impacted individuals. Note: even where there is no legal requirement, agencies may opt to notify affected individuals. Human Rights impact assessment to be carried out.	A summary of all notifications made by entities to to impacted cohorts must also be sent to: - - Irrelevant While the QGCSU/DJAG do not need individual copies of the notifications, the summary should include the following for WoQG centralised visibility and tracking: - # of notifications per cohort - Names of affected persons/organisations in each cohort
Organisations/third parties	2 – Qld Government to Organisation / Third Party	Contract manager or appropriately senior delegate	Affected entity completes harm assessment and determines where they would like to notify affected organisations/third parties of the breach for transparency and awareness (no legal compliance obligation). Complete template and send to impacted organisations/third parties.	
Staff	2 – Qld Government to Staff	Contract manager, Divisional Head, appropriately senior delegate	Affected entity completes harm assessment and determines where they would like to notify staff of the breach for transparency and awareness (no legal compliance obligation). Complete template and send to impacted staff.	

23

23

Draft letter – Individual

Dear xx

We are writing to advise you that HWL Ebsworth Lawyers (HWLE), a legal firm that the Queensland Government has regularly engaged to provide advice on legal cases and across several agencies, has experienced a significant cyber incident which has impacted [your personal] information. <<Agency / Organisation Name>> has worked with HWLE in recent years in relation to <<High level summary of services your Agency / Organisation has engaged HWLE on>>.

What happened?

HWLE recently informed the Queensland Government that the law firm was the victim of a criminal cyber-attack in April 2023, along with some Australian Government agencies and companies across Australia. Subsequent to further investigation by HWLE and other enforcement agencies into the data theft, HWLE has confirmed that some of [your personal information from the <<Agency / Organisation Name>>] that was held with HWLE has been taken as a result of this breach.

The following types of your personal information were identified as having been extracted from HWLE's network:

«Personal_Information_types_to_be_Input_Into_letters»

On 9 June 2023, we learnt that approximately one third of the data claimed to have been taken from HWLE had been published on the dark web that day. [insert status as to whether this individual's data has been published on the dark web].

What is the government doing in response?

The national Department of Home Affairs is leading the coordination effort in response to this incident. The Queensland Government is working with the Department of Home Affairs and multiple other agencies as part of the national response effort to provide support, assess potential consequences and minimise any harm. The Australian Signals Directorate's Australian Cyber Security Centre (ACSC), which leads the Australian Government's efforts to improve cyber security, including providing timely advice to individuals and businesses, is engaging with HWLE and is offering cyber security technical advice and assistance.

What happens next?

Once aware of the incident, we understand that HWLE worked urgently to contain the threat and investigate what occurred. HWLE also engaged external cyber security experts to assist with their response to the incident and is working with these experts to ensure the ongoing safety and security of its systems.

HWLE has informed us that it has reported the incident to and continues to work closely with the Australian Cyber Security Centre (ACSC), the Office of the Australian Information Commissioner (OAIC) as well as relevant government agencies and law enforcement authorities.

[details of other authorities/agencies - this might particularly include the ATO and Services Australia if TFNs, Medicare, Centrelink details are impacted].

24

24

Draft letter – Individual Cont.

Is my [personal data] information] with the Queensland Government safe?

We can confirm that neither <<Agency/Organisation's Name>> own systems nor the Queensland Government's systems have been impacted by this incident. As part of our duty to protect the data and privacy of all Queensland people and organisations, the Queensland Government deploys a range of cyber security measures to ensure the safety of your information.

What can impacted individuals do?

HWLE recommends individuals take the following steps to reduce the risk of harm associated with access to their personal information:

[Note: tailor to specific information impacted]

1. Remain alert to increased scam activity, especially email and SMS or telephone phishing scams (i.e., fraudulent communications disguised as if to look like they come from an organisation you trust) and, in particular any such scam activity purporting to come from HWLE or <<Organisation Name>>.
2. Do not click on any suspicious links or provide your passwords or any personal information. Always refuse any unprompted request from an individual to access to your computer even if they say they are from a credible organisation
3. Enable multi-factor authentication for your accounts where possible.
4. Consider changing your online account passwords. The Australian Cyber Security Centre provides guidance around good password practices: https://www.cyber.gov.au/acsc/view-all-content/advice/passwords-pins- and-passphrases;
   a. Install up-to-date anti-virus software on any device you use to access your online accounts; and
   b. To monitor your financial records, you can apply for an annual free credit report or credit report ban from each of the consumer credit reporting agencies below:
      i. Equifax: https://www.equifax.com.au/personal/products/credit-and-identity-products;
      ii. Illion: https://www.creditcheck.illion.com.au/; and
      iii. Experian: http://www.experian.com.au/consumer-reports

Where we have confirmed that your core identity information has been impacted (e.g. drivers licence, passport, birth certificate) HWLE is also willing to offer to you the option of taking out Equifax Credit Protect, a credit monitoring service that helps reduce the risk of financial loss, available for 12-months on request. This subscription includes alerts for changes to your credit reporting, monthly credit reports and score tracking. Should you wish to activate this subscription, please contact HWLE directly on Irrelevant to make the necessary arrangements.

25

25

Draft letter – Individual Cont.

Further information on online safety, cyber security and helpful tips to protect yourself and respond to scams, identity theft and other online risks, can be found at the following government agency websites:

- https://www.oaic.gov.au/privacy/your-privacy-rights/tips-to- protect-your-privacy/
- https://www.cyber.gov.au/acsc/view-all-content/threats
- https://www.scamwatch.gov.au/

IDCARE

If you need further assistance beyond the above recommendations, HWLE are making available to you the services of IDCARE, Australia's national identity and cyber support community service. HWLE has partnered with IDCARE specifically for the purpose of providing impacted individuals with tailored and specific advice, beyond the general advice that is ordinarily available to members of the public.

IDCARE have expert Case Managers who can work with you in addressing concerns in relation to personal information risks and any instances where you think your information may have been misused. IDCARE's services are at no cost to you.

If you wish to speak with one of IDCARE's expert Case Managers please complete an online Get Help form at www.idcare.org or call 1800 595160. Note IDCARE specialist Case Managers are available from 9am-6pm AEDT Monday to Friday excluding public holidays. When engaging IDCARE please use the referral code HWLEBS23.

Conclusion

The <<Queensland Government>> is deeply disappointed HWLE's IT environment was compromised. We would like to apologise for any concern or inconvenience this may cause you. The <<Queensland Government>> are closely monitoring their response, in concert with the Department for Home Affairs, and will seek to update you with further information, as necessary.

If you would like any more information about this incident, please contact us at [insert <<Organisation Name>> email address] and [phone] or you may contact HWLE directly on Irrelevant

Yours sincerely

26

26

Draft letter - Supplier

Dear xx

We are writing to advise you that HWL Ebsworth Lawyers (HWLE), a legal practice the Queensland Government has regularly engaged to provide advice on legal matters, across several agencies, has experienced a significant cyber incident which has impacted [name of organisation's confidential] information.

What happened?

HWLE recently informed the Queensland Government that the legal practice was the victim of a criminal cyber-attack in April 2023. Subsequent to further investigation by HWLE and other enforcement agencies into the data theft, HWLE has confirmed that some of your organisation's confidential information that was held with HWLE has been stolen as a result of this breach and may have been published on the dark web.

[NOTE: This is an initial letter from government with HWL Ebsworth to provide more detail, however agency may wish to provide more detail about the information, including about specific data that is confirmed as published]

Impacted Information

[Optional and modify as relevant: The stolen documents also contain work contact information of your staff such as name phone numbers and, in some cases, signatures. While this information does not include more sensitive personal information, we are notifying you of this to raise awareness of the potential increased risk of malicious phishing activities.

«Confidential_Information_types_to_be_input_into_letters»

What is the government doing in response?

The national Department of Home Affairs is leading the coordination effort in response to this incident. The Queensland Government is working with the Department of Home Affairs and multiple other agencies as part of the national response effort to provide support, assess potential consequences, and minimise any harm. The Australian Signals Directorate's Australian Cyber Security Centre (ACSC), which leads the Australian Government's efforts to improve cyber security, including providing timely advice to individuals and businesses, is engaging with HWLE and is offering cyber security technical advice and assistance.

What happens next? [REMOVE IF MAKING FULL NOTIFICATION]

As [name of organisation's] confidential information has been impacted by this cyber incident, HWLE will contact you directly to provide more detail about the cyber incident how it may have impacted your organisation and your staff or associated third parties, the measures that HWLE has taken and will take to protect the affected information, and the additional steps that you can take to protect [your organisation's confidential information].

Is [your organisation's information] with the Queensland Government safe?

We can confirm that neither <<Agency/Organisation's Name>> own systems nor the Queensland Government's systems have been impacted by this incident. As part of our duty to protect the data and privacy of all Queensland people and organisations, the Queensland Government deploys a range of cyber security measures to ensure the safety of your information

27

27

Draft letter – Supplier Cont.

What can I do now

You should always take steps to protect your information and avoid any potential scams. Stay up to date on cyber security threats and trends with ACSC Alert Service and advice to protect your information by visiting cyber.gov.au.

In addition to this, if your staff have any concerns about the disclosure of their personal information, they can contact IDCare (https://www.idcare.org/) or phone on 1800 595 160 for further assistance. IDCare has provided expert advice, support and guidance to individuals affected by a number of recent data breaches including Optus and Medibank. When engaging IDCARE please use the referral code HWLEBS23.

The Office of the Queensland Information Commissioner (OIC) has published advice for individuals on how to reduce risks of harm following a data breach which is readily available on the OIC's website: www.oic.qld.gov.au

Current advice from HWL Ebsworth

Independent cyber security experts have examined the HWLE systems and confirmed that they are secure. There has been no further unauthorised activity detected.

Conclusion

We want to assure you that protecting your privacy, and the confidentiality of your/your organisation's data and information is of the Queensland Government's highest priority, and we wish to assure you that we will continue to work with HWLE, national response agencies and independent cyber security advisors to do everything we can to minimise the impact of this cyber incident.

If you would like any more information about this incident, please contact us at [insert <<Organisation Name>> email address] and [phone] or you may contact HWLE directly on Irrelevant

Yours Sincerely

28

28

Draft letter - Staff

We are writing to advise you that HWL Ebsworth Lawyers (HWLE), a legal practice the Queensland Government has regularly engaged for advice across several agencies, has experienced a significant cyber incident which has impacted your personal information.

What happened?

HWLE recently informed the Queensland Government that the legal practice was the victim of a criminal cyber-attack in April 2023. After further investigation by HWLE and other enforcement agencies into the data theft, HWLE has confirmed that certain specific information was stolen as a result of this breach and may have been published on the dark web.

HWLE have contained the breach and independent cyber security experts have confirmed that their systems are now secure. There has been no further unauthorised activity detected.

What information has been published?

The information is primarily routine work information, such as:

- your name
- position
- work location,
- direct and mobile phone numbers
- work email address
- In some cases signatures have also been impacted.

What will happen next? / What can I do ? [REMOVE/ADAPT IF MAKING FULL NOTIFICATION]

HWLE will contact you directly to provide a formal notification of the breach including how to make a privacy complaint if you desire.

In the meantime, if you feel concerned about your situation, please contact ID Care (https://www.idcare.org/) or phone on 1800 595 160 for further assistance. IDCare is a national identity and cyber support service and has provided expert advice and guidance to individuals affected by recent data breaches including Optus and Medibank. When engaging IDCARE please use the referral code HWLEBS23.

You are also encouraged to take additional steps to protect yourself from potential increases in scam activity, such as:

- Change your passwords on any online/mobile phone apps that use the compromised email address.
- Don't open links in emails or text messages that look suspicious. Scamwatch (scamwatch.gov.au) provides more information about email and text message scams
- You may want to contact your mobile phone provider if you think someone might be using the compromised number.
- Update your device and turn on automatic updates to ensure you always have the most up-to-date security protection.
- Always use multi-factor authentication to increase the security of your accou and make it harder for criminals to gain initial access to your device

29

29

Draft letter - Staff

NOTE: Agency to amend following paragraph as appropriate

[You can also access the Employee Assistance Service (EAS) available to Queensland Health staff. Information about the service, including contact details, is available at https://qheps.health.qld.gov.au/csd/employee-centre/work/health-safety-wellbeing/employee-assistance-service-providers.]

Conclusion

The Queensland Government is deeply disappointed HWLE's IT environment was compromised. We apologise for any inconvenience arising from this breach and want to assure you that protecting your privacy, and the confidentiality of your data and information is of the Queensland Government's highest priority. We are continuing to work with HWLE, national response agencies and independent cyber security advisors to do everything we can to minimise the impact of this cyber incident.

If you would like any more information about this incident, please contact us at [insert <<Organisation Name>> email address] and [phone] or you may contact HWLE directly on Irrelevant

Yours Sincerely

30

30

31

Irrelevant

From: Michelle Wellington (DPC)
Sent: Friday, 14 July 2023 4:54 PM
To: Mike Kaiser (DSDILGP); Mike Kaiser
Cc: Michael Carey; Rebecca McGarrity; Kyla Hayden; Emmy Kubainski; Julia Sheedy; Emma Kinnane
Subject: FW: Seeking approval - urgent - Media request: Guardian Aus - HWL Ebsworth Data Breach. (short timeline provided by journalist)

Hi Mike

For awareness, the Transport Minister's office has received an enquiry re the HWL Ebsworth data breach. Question and response provided are in the email below.

Media interest to date has been minimal.

Kind regards

Michelle Wellington (She/Her)
Assistant Director-General
Reform and Delivery
Department of the Premier and Cabinet
M: Irrelevant
E: michelle.wellington@premiers.qld.gov.au
1 William Street, Brisbane QLD 4000
PO Box 15185, City East, QLD 4002

Queensland Government

NB: I sometimes work and send correspondence out of hours. Please do not feel obliged to respond outside of your own work hours.

Queensland Good jobs Better services Great lifestyle

From: Nicole Z Davis <Nicole.Z.Davis@tmr.qld.gov.au>
Sent: Friday, July 14, 2023 3:43 PM
To: Michelle Wellington (DPC) <michelle.wellington@premiers.qld.gov.au>; Emmy Kubainski <emmy.kubainski@premiers.qld.gov.au>
Cc: Tracey Walker <Tracey.Walker@health.qld.gov.au>; Danielle Mahl <Danielle.Mahl@cyber.chde.qld.gov.au>; James Murphy (TMR) <James.X.Murphy@tmr.qld.gov.au>; Media (TMR) <Irrelevant>
Subject: FW: Seeking approval - urgent - Media request: Guardian Aus - HWL Ebsworth Data Breach. (short timeline provided by journalist)

Hi Team,

FYI The following is about to be provided to Mins office to provide to Guardian with DG approval.

It includes the pre-approved response from pack.

Office of the Information was also approached by the Guardian and has referred them to us.

Nic Davis
Executive Director, Strategic Communication Unit
Governance Branch | Corporate Division | Department of Transport and Main Roads

I work flexibly at TMR. I'm sending this message now because it suits my working arrangements. I don't expect you to read, action or respond out of your normal work hours.

Floor 8 | 61 Mary Street | Brisbane Qld 4000
GPO Box 1549 | Brisbane Qld 4001
P: (07) 3338 4129| M: Irrelevant
E: nzdavis@tmr.qld.gov.au
W: www.tmr.qld.gov.au

The Department of Transport and Main Roads acknowledges the Traditional Owners and Custodians of thi
We also acknowledge their ancestors and Elders both past and present.
The Department of Transport and Main Roads is committed to reconciliation among all Australians.

Media Enquiry

1. Is the Qld government aware of any sensitive government information being stolen and leaked to the dark web as a result of the HWL Ebsworth hack?
2. The law firm has clients at government level in every state and territory. Is Queensland concerned about reports that Victorian government information has been stolen?
3. What action has the government taken to respond to this cyber attack?

Our preapproved response for this inquiry is below. This is email is to confirm that you are ok for us to provide to The Guardian.
This has been approved by QGCD and Heads of Legal across all government departments. I have attached the pre approved comms pack again for your information.
I will also circulate the email request and response to Prems prior to providing to MO if ok with you.

Whole of Queensland Government Response

- On 8 May 2023, HWL Ebsworth reported a data breach to the Office of the Australian Information Commissioner (OAIC) under the Notifiable Data Breaches (NDB) scheme.
- HWL Ebsworth advised the Queensland Government that documents relating to a limited number of Department's files were included in the breach experienced by HWL Ebsworth.
- The Department of Home Affairs continues to work with HWL Ebsworth and affected Government agencies as it investigates the extent of the breach, including exposure of Queensland Government information and related consequences arising from this exposure.
- The Queensland Government takes the privacy of its data holdings seriously and is working with HWL Ebsworth to understand what information may have been disclosed.
- Should our clients' personal information be affected, the individual Departments will work with HWL Ebsworth to ensure affected individuals are notified as soon as possible, and offer assistance and support as required.
- The Queensland Government is committed to ensuring appropriate systems are in place to maintain the privacy and the protection of personal information.
- Queensland Government systems have not been compromised.

Many thanks

Nic

Nic Davis
Executive Director, Strategic Communication Unit
Governance Branch | Corporate Division | Department of Transport and Main Roads

I work flexibly at TMR. I'm sending this message now because it suits my working arrangements.
I don't expect you to read, action or respond out of your normal work hours.

Floor 8 | 61 Mary Street | Brisbane Qld 4000
GPO Box 1549 | Brisbane Qld 4001
P: (07) 3338 4129| M: Irrelevant
E: nzdavis@tmr.qld.gov.au
W: www.tmr.qld.gov.au

The Department of Transport and Main Roads acknowledges the Traditional Owners and Custodians of thi
We also acknowledge their ancestors and Elders both past and present.
The Department of Transport and Main Roads is committed to reconciliation among all Australians.

From: Lesley Major <Lesley.Major@ministerial.qld.gov.au>
Sent: Friday, 14 July 2023 1:41 PM
To: Media < Irrelevant >
Cc: Charlton Hart <Charlton.Hart@ministerial.qld.gov.au>; James X Murphy <James.X.Murphy@tmr.qld.gov.au>; Nicole Z Davis <Nicole.Z.Davis@tmr.qld.gov.au>
Subject: FW: Media request: Guardian Aus

Hi team

Could I please get a response to the below.

Thanks

Irrelevant

Irrelevant

From: Rebecca McGarrity
Sent: Thursday, 31 August 2023 9:38 AM
To: Tam van Alphen
Cc: Rachel Hunter;Michael Carey
Subject: Update: Situation Report 11 - Law Firm HWL Ebsworth Cyber Incident and Data Breach [OFFICIAL:SENSITIVE + LEGAL PRIVILEGE]

Hello Tam – FYI.

The Cyber Security Unit in TMR has provided an update on the HWL Ebsworth (HWLE) cyber incident/data breach (**attached** sit rep with more detail).

Key updates

- HWLE have now issued final reports to all affected Queensland Government agencies, and of those impacted only **three agencies** have identified documents that carry an **obligation** to notify those affected to manage the risk of serious harm: Office of Industrial Relations (OIR); Queensland Revenue Office (QRO); and Department of Transport and Main Roads (DTMR).
- **These agencies are in the process of finalising harm assessments and planning for notification which continues to occur on an agency by agency basis in alignment with a WoG approach following completion of harm assessment, with notifications commencing today 30 August 2023.**
- While other impacted agencies have **no legal obligation** to notify impacted staff and suppliers (as they have not been assessed to be at risk of serious harm) many have opted to make proactive notifications: 1. to ensure staff are cyber aware, have support and where to seek information; and 2. to advise suppliers of the type of information compromised so they can take action to protect their systems and organisation. Agency reporting to date identifies that proactive notifications have been issued to a total of 71 impacted staff and 22 suppliers. To date no significant complications or concerns have arisen following the issue of proactive notifications by agencies.

Media

- At this time, **no media** on the breach has focused on or mentioned Queensland government agencies, though this may change as notifications commence. To ensure visibility and appropriate action, Queensland Government agencies have been asked to forward any media queries to DTMR Strategic Communications Unit to coordinate.

Rebecca McGarrity PSM
Deputy Director-General
Policy Division
Department of the Premier and Cabinet
T 300 39156 M Irrelevant
Level 30, 1 William Street, Brisbane QLD 4000
PO Box 15185, City East, QLD 4002
Queensland Government

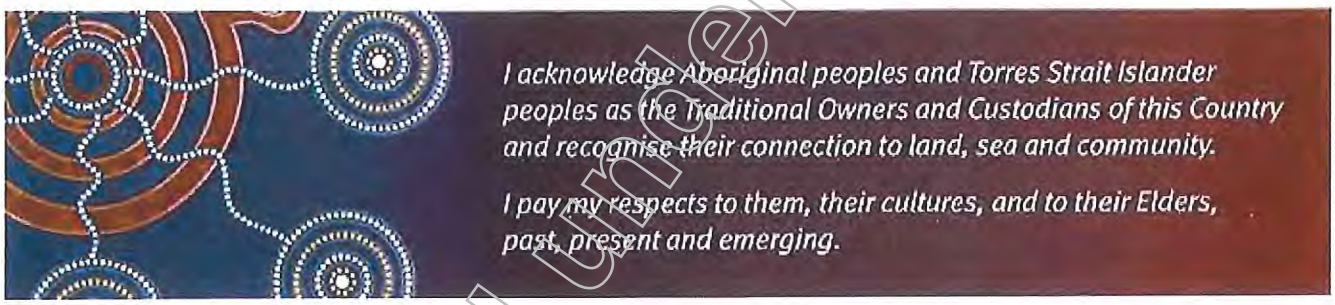
Irrelevant

From: Filly Morgan
Sent: Friday, 27 October 2023 1:23 PM
To: Rachel Hunter
Cc: Emma Kinnane;Jayne Hartley
Subject: FW: For Information: 27 October 2023 Cyber incident - Service outage currently impacting Queensland Government cyber services - for your information
Attachments: HIB - SSQ + Squiz.docx

Importance: High
Sensitivity: Confidential

Fyi.

Filly Morgan
Associate Director-General
Governance and Engagement
Department of the Premier and Cabinet
P 07 3003 9224 M Irrelevant
Level 28, 1 William Street, Brisbane QLD 4000
PO Box 15185, City East, QLD 4002
Queensland Government



From: Libby Gregoric <libby.gregoric@premiers.qld.gov.au>
Sent: Friday, October 27, 2023 1:20 PM
To: Kristen Foster <kristen.foster@premiers.qld.gov.au>; Prue Laven <prue.laven@premiers.qld.gov.au>
Cc: Filly Morgan <filly.morgan@premiers.qld.gov.au>; Jayne Hartley <jayne.hartley@premiers.qld.gov.au>; Scott Mathewson <scott.mathewson@premiers.qld.gov.au>; Kylie Anderson <kylie.anderson@premiers.qld.gov.au>
Subject: FW: For Information: 27 October 2023 Cyber incident - Service outage currently impacting Queensland Government cyber services - for your information
Importance: High
Sensitivity: Confidential

FYI all

Regards

Libby

Libby Gregoric

Deputy Director-General

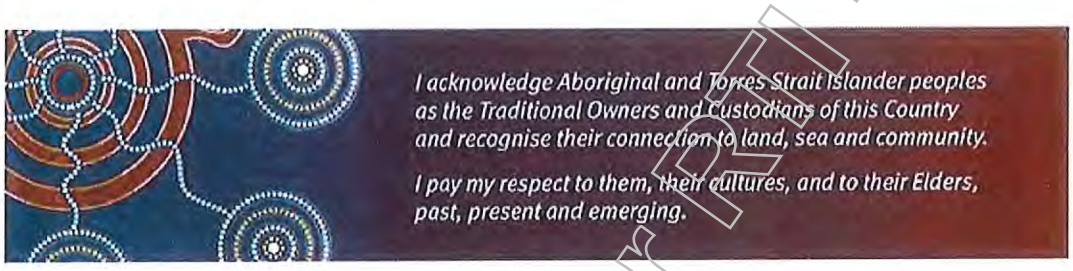
People and Services

Department of the Premier and Cabinet

P 07 3003 9046 M Irrelevant

Level 28, 1 William Street, Brisbane QLD 4000

PO Box 15185, City East, QLD 4002



From: Michelle Jackson-Hay <Michelle.Jackson-Hay@premiers.qld.gov.au>
Sent: Friday, October 27, 2023 10:56 AM
To: Rebecca McGarrity <rebecca.mcgarrity@premiers.qld.gov.au>; Michelle Wellington (DPC) <michelle.wellington@premiers.qld.gov.au>; Libby Gregoric <libby.gregoric@premiers.qld.gov.au>
Cc: Sally Lohrisch <sally.lohrisch@premiers.qld.gov.au>; Matthew Byrnes <matthew.byrnes@premiers.qld.gov.au>; Tammy Woolf-Stefanutto <tammy.woolf-stefanutto@premiers.qld.gov.au>
Subject: For Information: 27 October 2023 Cyber incident - Service outage currently impacting Queensland Government cyber services - for your information
Importance: High
Sensitivity: Confidential

Good morning Rebecca, Michelle and Libby

For your awareness, please be advised that the Cyber Security Unit (TMR) has given us an early heads up for our awareness around a cyber incident impacting some Qld Government web services, in particular SSQ. The attached HIB from SSQ and information below should be treated confidentially and we have been asked to please limit distribution of this information only to key personnel within DPC.

For your noting, anecdotally I've done some informal checks of the web domains listed below and have been able to access these services – noting the intermittent nature of the disruption. The key point from the brief attached is that the impact is currently understood to be that users may be experiencing slow response time or not be able to access service, intermittently.

The CSU have indicated that there will likely be a WoG focused situation update later today, but providing the below information around the current situation just for awareness.

Background

- Sch 1 of the RTI Act - Security Document

Qld/Qld Gov Impacts

- A service outage is currently impacting the below Queensland Government cyber services.
  - Qld.gov.au
  - Disaster.qld.gov.au
  - Forgov.qld.gov.au
  - Qld Alerts
  - Open Data Portal
- The issue was identified at 5:40am Friday 27 October.
- Users may be experiencing slow response time or not be able to access service, intermittently.
- In addition to the service above which are managed by Customer and Digital group, other government users are also experiencing impacts. These are currently known to include (but are not limited to) Queensland Health and the Department of Energy and Public Works.
- While the cause of the issue is being confirmed and claims are emerging, DDoS activity has been observed in other Australian jurisdictions (some also linked to Squiz, but some separate to) overnight and into the morning.

Impact in other Australian jurisdictions

- Impacts in other jurisdictions have also been limited to website disruption. Jurisdictions include the ACT, Victoria and the NT. Other jurisdictions are also investigating.
- Jurisdictions are investigating in partnership with the ACSC, which is working to engage with Squiz.

- Collective intelligence arising is being circulated among jurisdictions via the National Cyber Security Operations Sub-Committee as it becomes available.

Suggested Media Response / Holding Statement

- We are aware of intermittent issues with qld.gov.au which may be impacting some on line services.
- We are working with the service provider to resolve the situation.
- In the interim please contact 13QGOV for assistance if required.

Kind regards

Michelle Jackson-Hay (She/Her)

Director, Law and Justice Policy

The Cabinet Office

Department of the Premier and Cabinet

P 07 3003 9033 M Irrelevant

Level 30, 1 William Street, Brisbane QLD 4000

PO Box 15185, City East, QLD 4002

Mon	Tue	Wed	Thu	Fri
1WS		1WS		1WS

Please note: I sometimes work and send correspondence out of hours. Please do not feel obliged to respond outside of your own work hours.

From: Danielle Mahl <Danielle.Mahl@cyber.chde.qld.gov.au>
Sent: Friday, October 27, 2023 9:52 AM
To: Matthew Byrnes <matthew.byrnes@premiers.qld.gov.au>
Subject: As discussed

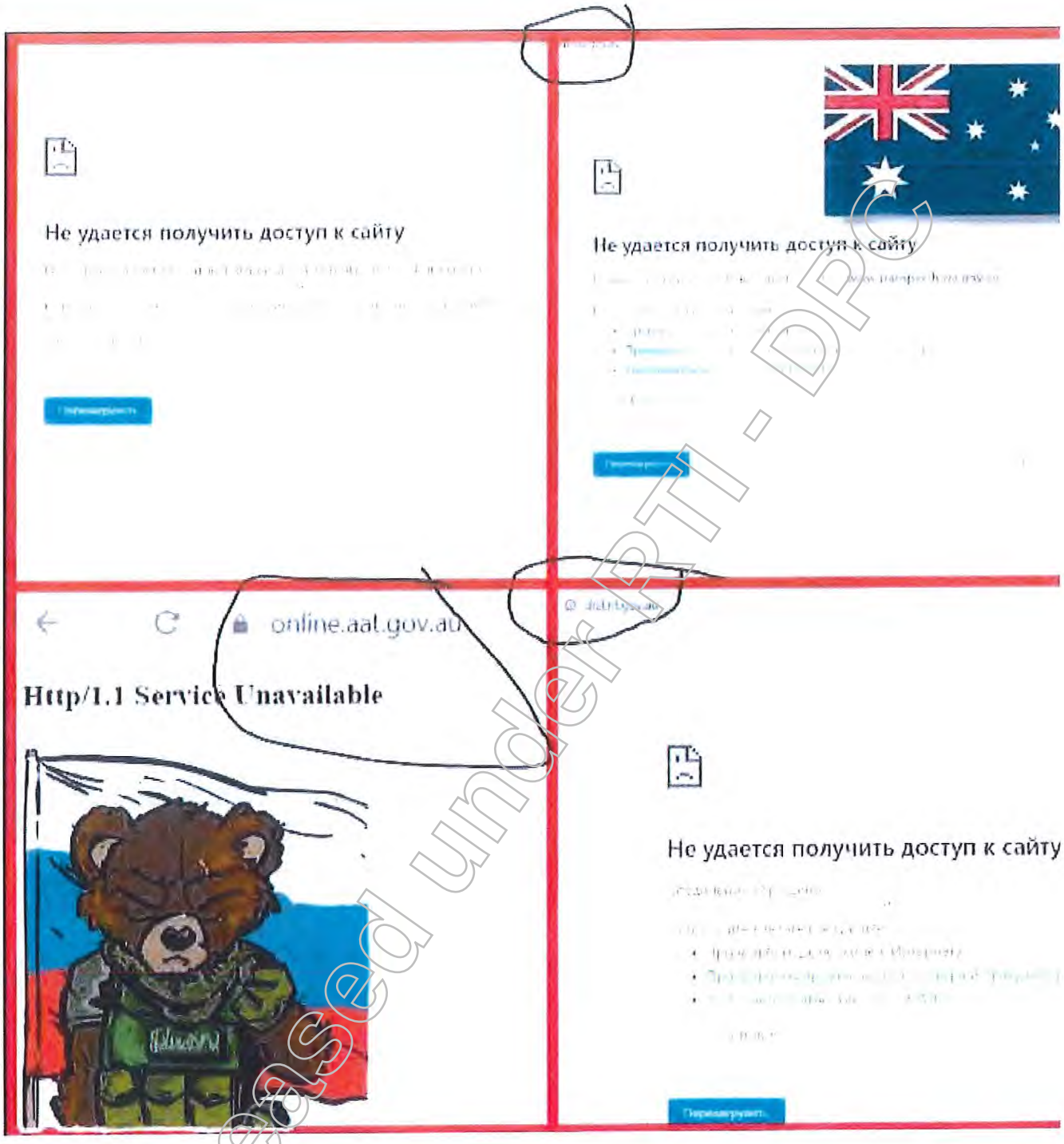
Hi Matt,

As discussed, SSQ HIB Attached (cyber currently not leading but providing input). Additional advice below for DPC awareness only and not for further distribution at this time (TLP Red, ACSC controlled).

I have asked the QGISVRT and SSQ to summarise current QGov impacts and send it through. I also have a NOSC bridge later today and will work with the applicable teams to provide a situation update.

Sch 1 of the RTI Act - Security Document

2023-10-26 10:06:16	#Australian authorities are sending a new package of military aid to K ngs" of Western Russophobes lead only to the trophying of military equ But all this is on the money of honest taxpayers, whose opinion is not e ng to Australia for destroying portals of critical infrastructure!AU A ransport in Perth:check-host.net/check-report/12cae7b0k80d Depar 12cae94bke2e Court of Appeal:Auth - check-host.net/check-report/



Kind Regards,

Danielle Mahl

Manager - Incident Response and Communications

Queensland Government Cyber Security Unit

Department of Transport and Main Roads.
Level 5 | 140 Creek Street | Brisbane
ph Irrelevant **email** danielle.mahl@cyber.chde.qld.gov.au

27 October 2023

Hot issues brief (HIB)

Service Outage: Qld.gov.au

Media Response / Holding Statement

We are aware of intermittent issues with qld.gov.au which may be impacting some on line services.

We are working with the service provider to resolve the situation.

In the interim please contact 13QGOV for assistance if required.

Social media messaging

Not applicable.

Background

- A service outage is currently impacting the below Queensland services.
    - Qld.gov.au
    - Disaster.qld.gov.au
    - Forgov.qld.gov.au
    - Qld Alerts
    - Open Data Portal
- The issue was identified at 5:40am Friday 27 October.
- Users may be experiencing slow response time or not be able to access service, intermittently.
- In addition to the service above which are managed by Customer and Digital group, other government users using their own instance of Squiz are also experiencing impacts. These currently known to include (but are not limited to) Queensland Health and the Department of Energy and Public Works.
- While the cause of the issue is being confirmed and claims are emerging, Suspected Distributed Denial-of-Service (DDoS) activity has been observed in other jurisdictions (some also linked to Squiz, but some separate to) overnight and into the morning.

- Impacts in other jurisdictions have also been limited to website disruption.
- Jurisdictions include the Australian Capital Territory, Victoria and the Northern Territory. Other jusrisidictions are also investigating.
- Respective jurisdictions are investigating in partnership with the Australian Cyber Security Centre, who are working to engage with Squiz.
- Collective intelligence arising is being circulated among jurisdictions via the National Cyber Security Operations Sub-Committee as it becomes available.

Prepared by:	*Document author*	**Contact for further information:**	*Content expert*
Danielle Mahl	*Manager – Incident Response and Communications*	*Robert Champion*	*Queensland Government Chief Information Security Officer*

Irrelevant

From: Michelle Wellington (DPC)
Sent: Saturday, 11 November 2023 8:12 PM
To: Premiers Media;Jim Murphy (Ministerial);Mike Kaiser (DSDILGP);Rachel Hunter;Jessica Collins;Rebecca McGarrity
Cc: Emmy Kubainski
Subject: WofG Talking Points - DP World cyber incident - v1 [SEC=OFFICIAL]
Attachments: 231111 Talking points - DP World Australia cyber incident - v1.docx

Importance: High

Good evening

Please find attached Commonwealth Talking Points related to the DP World Australia cyber incident (v1).

Below is a HIB from TMR. PLs note: there have been no media enquiries received at this point.

11 November 2023

Hot issues brief (HIB) – Update 1

Cyber incident affecting DP World Australia

Media Response / Holding Statement

- The Queensland Government is aware of reports of a cyber incident affecting DP World Australia.
- We continue to remain on alert and monitor the situation to understand the impacts to Qld Government and Queenslanders.
- The Port of Brisbane remains open and operational, with the DP World container terminal the only terminal affected at this stage.
- Maritime Safety Queensland continues to monitor and oversee safe and efficient port operations in Port Brisbane and coastal shipping at the approaches to the Port
- At this stage there are no signs of ingress into our Maritime Safety Queensland (MSQ) systems or internal environments.
- Specific enquiries relating to this incident should be directed to DP World Australia.

Social media messaging

Not applicable.

Background (OFFICIAL SENSITIVE – NOT PUBLIC INFORMATION TO BE USED FOR ENGAGEMENT WITH DP WORLD AUSTRALIA)

- Sch 1 of the RTI Act - Security Document

Sch 1 of the RTI Act - Security Document

Kind regards

Michelle Wellington (She/Her)
Assistant Director-General
Reform and Delivery
Department of the Premier and Cabinet
M: Irrelevant
E: michelle.wellington@premiers.qld.gov.au
1 William Street, Brisbane QLD 4000
PO Box 15185, City East, QLD 4002

Queensland Government

NB: I sometimes work and send correspondence out of hours. Please do not feel obliged to respond outside of your own work hours.

Queensland Good jobs Better services Great lifestyle

From: Crisis Media Operations <Irrelevant>
Sent: Saturday, November 11, 2023 6:22:08 PM
To: Crisis Media Operations <Irrelevant>
Subject: WofG Talking Points - DP World cyber incident - v1 [SEC=OFFICIAL]

EXTERNAL

OFFICIAL

Good evening,

Please find attached version 1 of the Whole of Government talking points for the DP World cyber incident.

These will continue to be updated and reissued as required. If your agency wishes to provide input/changes, please send this through to Irrelevant

Thanks

Alex

Alex McConachie
A/g Director, Cyber Communications
Media and Communication Branch | Executive Coordination Division
Executive Group
Department of Home Affairs
Media Line: 02 6264 2244 | **P:** 02 6198 7034 | **M** Irrelevant
E: alex.mcconachie@homeaffairs.gov.au

OFFICIAL

********** Disclaimer **********

TALKING POINTS

Subject	DP World Australia Cyber Security Incident	
Date	11 November 2023	
Type	Whole of Government	
Media Officer: Alex McConachie		**Media Ph:** 02 6264 2244

ISSUE

Cyber incident impacting ports operator DP World Australia.

TALKING POINTS

- The Australian Government is aware of a cyber incident impacting ports operator, container terminal and supply chain logistics provider, DP World Australia.
- DP World Australia is actively working with relevant parts of the Australian Government and local authorities and suppliers to resolve the issue.
- There will be significant impacts to DP World Australia's operations over the coming week as the company seeks to resolve the cyber incident and its impact to their operations.
- DP World Australia has advised that its teams are working "diligently to contain the situation and determine the impact on our systems and data."
- DP World Australia has also advised that in order to safeguard its workers, systems and networks it has also restricted access to its Australian port operations in the Port of Botany, Port of Melbourne, Port of Brisbane, Port of Fremantle while it investigates the incident.
    - DP World Australia has advised this restriction is likely to continue into next week as it seeks to resolve the cyber incident.
- DP World Australia is a Port Facility Operator under the *Maritime Transport and Offshore Facilities Act 2003 (MTOFSA).*
- DP World Australia operates in four critical ports as defined by the *Security of Critical Infrastructure Act 2018* located at Port of Botany, Port of Melbourne, Port of Brisbane and Port of Fremantle.
- The National Cyber Security Coordinator is working closely with DP World Australia to understand the impacts of this incident and to facilitate engagement across government.
- The National Office of Cyber Security is leading the coordination effort to manage potential consequences that may be realised from this incident.
- The National Coordination Mechanism (NCM) was jointly convened by the National Cyber Security Coordinator and the National Emergency Management Agency on 11 November 2023.

- The NCM was attended by key representatives from the Australian, state and territory governments, as well as the maritime and logistics sectors.
- DP World Australia provided an update on the incident, the impact on their operations and the response.

- The Cyber and Infrastructure Security Group in the Department of Home Affairs will work with other maritime, freight and logistics providers throughout the incident to support the work of the National Coordination Mechanism and any future lessons learned to harden the maritime environment from cyber attacks.
- The Australian Signals Directorate's Australian Cyber Security Centre (ACSC) is engaging DP World Australia and providing technical advice and assistance as required.
- The Australian Federal Police has commenced an investigation into this incident.
- Specific enquiries relating to this incident should be directed to DP World Australia.

CLEARANCE

Lead business area
Cyber Security Response Coordination Unit
Cyber and Infrastructure Security Group

Drafting officer		
Alex McConachie	A/g Director, Cyber Communications	11/11/2023

Other Government agency consultation/clearance	**Yes ☒ N/A ☐**
Australian Signals Directorate	11/11/2023
Australian Federal Police	11/11/2023
National Emergency Management Agency	11/11/2023

Final SES clearance (minimum SES Band 1) and approval for release

AM Darren Goldie AM CSC	National Cyber Security Coordinator	11/11/2023

Media and Communication Branch		
Alex McConachie	A/g Director, Cyber Communications	11/11/2023

Irrelevant

From: NGComms Irrelevant > on behalf of State Disaster Coordination Centre < Irrelevant
Sent: Monday, 13 November 2023 5:00 AM
To: Rachel Hunter
Subject: QEMR as at 13/11/2023 05:00
Attachments: QEMR as at 13-11-2023 05_00.pdf

Categories: Reporting/Media

Dear Ms Rachel Hunter,

Please find attached the Queensland Emergency Management Report as at 13/11/2023 05:00.

If you no longer wish to receive the Queensland Emergency Management Report, please reply to this email and detail which email address you would like removed from the distribution list.

If you require any further information, please contact the SDCC Watch Desk as undersigned.

Regards,

State Disaster Coordination Centre | Watch Desk
Queensland Fire and Emergency Services
Level 2, State Disaster Management Centre, Kedron
GPO Box 1425 Brisbane QLD 4001
P: 07 3635 2387 (24hrs) | M: Irrelevant
F: 07 3357 4682 | E: Irrelevant

Queensland Emergency Management Report

Report Time	13/11/2023 05:00	Report ID	R32349122

Emergency and Disaster Management Operations

Queensland

- Irrelevant
- The Brisbane port remains operational however DP World continue to work through the impacts from the recent cyber security incident and their operations have reportedly not yet restarted in Brisbane.

Australia

-

International

-

Major Infrastructure Advice

Traffic Updates and Alerts / Rail / Marine

Major Roads and Arterials

Airports, Rail and Marine Ports

Major Power Outages

Critical Infrastructure

Weather

Forecast for Today

Current

Warnings

Rainfall Since 0900 Yesterday

Operational Activity

Disaster Management

QFES Significant Operations

Irrelevant

Queensland Government

Irrelevant

- Irrelevant

Current Status of Activations

Media

Full access to some media articles in this report may require a digital subscription

Source	Details

Queensland Government

Irrelevant

Reuters	Australia says ports operator cyber incident 'serious': DP World Australia, which manages nearly half of the goods that flow in and out of the country, said it was looking into possible data breaches as well as testing systems "crucial for the resumption of normal operations and regular freight movement".

Next Report

The next Queensland Emergency Management Report will be issued at 0500 hours tomorrow.

The QEMR is issued under the authority of the
Director, State Operational Coordination Branch, Queensland Fire and Emergency Services

SDCC Watch Desk

The State Disaster Coordination Centre Watch Desk operates on a 24-hour capability and can be contacted as undersigned for further information.

The SDCC Watch Desk is responsible for reporting on emergency and disaster management activities and providing situational awareness to enhance decision making for emergency management, disaster management and senior QFES stakeholders.

Some information is obtained from unofficial sources and may not have been verified.

State Disaster Coordination Centre
125 Kedron Park Road
Kedron Queensland 4031
Telephone: (07) 3635 2387
Fax: (07) 3357 4682
Email: Irrelevant

Queensland Government

Irrelevant

From: Michelle Wellington (DPC)
Sent: Monday, 13 November 2023 5:05 PM
To: Premiers Media;Jim Murphy (Ministerial);Jessica Collins;Rachel Hunter;Rebecca McGarrity
Cc: Emmy Kubainski;Michelle Jackson-Hay;Sally Lohrisch;Crisis Coordination
Subject: Fwd: WofG Talking Points - DP World Aus cyber incident - V3 - 13 November 2023 [SEC=OFFICIAL]
Attachments: WoG Talking points - DP World Australia cyber incident - v3.docx

Categories: Reporting/Media

Good afternoon

Updated Commonwealth Talking Points related to DP World (v3).

Kind regards

Michelle Wellington

Get Outlook for iOS

From: Crisis Media Operations <Irrelevant>
Sent: Monday, November 13, 2023 5:02:40 PM
To: Crisis Media Operations <Irrelevant>
Subject: WofG Talking Points - DP World Aus cyber incident - V3 - 13 November 2023 [SEC=OFFICIAL]

OFFICIAL

Good afternoon,

Please find attached version 3 of the Whole of Government talking points for the DP World Australia cyber incident.

These talking points will continue to be updated and reissued as required. If your agency wishes to provide input/changes, please send this through to Irrelevant

Kind regards,

Hayley

National Security and Crisis Communication
Department of Home Affairs
Crisis media on-call: M: Irrelevant **E:** Irrelevant

OFFICIAL

TALKING POINTS

Subject	DP World Australia Cyber Security Incident – version 3	
Date	13 November 2023	
Type	Whole of Government	
Media Officer: Hayley Scott		**Media Ph:** 02 6264 2244

ISSUE

Cyber incident impacting ports operator DP World Australia.

TALKING POINTS

- DP World Australia has resumed operations today following the cyber incident that impacted a number of ports around the country.
    - The Australian Government is continuing to work with DP World Australia to support the management of any further consequences, including any ongoing disruption to Australia's supply chains.
    - Although port operations have resumed, it does not mean that this incident has concluded.
- There will continue to be impacts to DP World Australia's operations as the company seeks to remediate the cyber incident and its disruption to their operations.
- DP World Australia has advised the ongoing investigation and response may cause some necessary, temporary disruptions to services in the coming days.
    - This is a part of an investigation process and resuming normal logistical operations at this scale.
- DP World Australia is a Port Facility Operator under the *Maritime Transport and Offshore Facilities Act 2003 (MTOFSA).*
- DP World Australia operates in four critical ports as defined by the *Security of Critical Infrastructure Act 2018* located at Port of Botany, Port of Melbourne, Port of Brisbane and Port of Fremantle.
- The National Coordination Mechanism (NCM) was jointly convened by the National Cyber Security Coordinator and the National Emergency Management Agency on 11 and 12 November 2023.
    - The NCM was attended by key representatives from the Australian, state and territory governments, as well as the maritime and logistics sectors.
    - DP World Australia provided an update on the incident, the impact on their operations and the response.

- A further NCM was held on 13 November to consider the freight and logistic consequences from this incident.
- At this stage, no further NCM meetings are planned.

- The Cyber and Infrastructure Security Group in the Department of Home Affairs is working with other maritime, freight and logistics providers to support the work of the National Coordination Mechanism and any future lessons learned to harden the maritime environment from cyber attacks.
- DP World has proactively engaged with the Office of the Australian Information Commissioner (OAIC) on the incident.
- The Australian Signals Directorate's Australian Cyber Security Centre (ACSC) is engaging DP World Australia and providing technical advice and assistance as required.
- The Australian Federal Police investigation into this incident continues.
- Specific enquiries relating to this incident should be directed to DP World Australia.

CLEARANCE

Lead business area
Cyber Security Response Coordination Unit
Cyber and Infrastructure Security Group

Drafting officer		
Hayley Scott	Public Affairs Officer	13/11/2023

Other Government agency consultation/clearance	**Yes ☒ N/A ☐**
Australian Signals Directorate	11/11/2023
Australian Federal Police	11/11/2023
National Emergency Management Agency	11/11/2023
Office of the Australian Information Commissioner	12/11/2023

Final SES clearance (minimum SES Band 1) and approval for release

AM Darren Goldie AM CSC	National Cyber Security Coordinator	13/11/2023

Media and Communication Branch		
Tracy Heffernan	Director, National Security and Crisis Communications	13/11/2023

Irrelevant

From: Filly Morgan
Sent: Thursday, 16 November 2023 11:05 AM
To: Rachel Hunter
Subject: Fwd: ESCALATION ADVICE - Queensland Government Cyber Security Arrangements

Categories: Rachel

FYI

Sent from my iPhone

Begin forwarded message:

> **From:** Libby Gregoric <libby.gregoric@premiers.qld.gov.au>
> **Date:** 16 November 2023 at 11:02:44 am AEST
> **To:** Filly Morgan <filly.morgan@premiers.qld.gov.au>
> **Cc:** Ella Bailey <ella.bailey@premiers.qld.gov.au>
> **Subject: FW: ESCALATION ADVICE - Queensland Government Cyber Security Arrangements**
>
> OFFICIAL
>
> FYI
>
> Patches are in place
>
> Regards
>
> Libby

Queensland Government Libby Gregoric
Deputy Director-General
People and Services
Department of the Premier and Cabinet
P 07 3003 9046 M Irrelevant
Level 28, 1 William Street, Brisbane QLD 4000
PO Box 15185, City East, QLD 4002

From: Libby Gregoric <libby.gregoric@premiers.qld.gov.au>
Sent: Wednesday, November 15, 2023 4:29 PM
To: Leigh Dixon <leigh.dixon@premiers.qld.gov.au>; Kristen Foster <kristen.foster@premiers.qld.gov.au>; Scott Mathewson <scott.mathewson@premiers.qld.gov.au>; Pamela Healy <pamela.healy@premiers.qld.gov.au>; Michael Phillips <Michael.Phillips@premiers.qld.gov.au>
Cc: Steven Wishart <steven.wishart@premiers.qld.gov.au>
Subject: Re: ESCALATION ADVICE - Queensland Government Cyber Security Arrangements

Thanks Leigh. L

Libby Gregoric
Deputy Director-General
People and Services
Department of the Premier and Cabinet
P: 07 3003 9046 M: Irrelevant
E: Libby.Gregoric@premiers.qld.gov.au

From: Leigh Dixon <leigh.dixon@premiers.qld.gov.au>
Sent: Wednesday, November 15, 2023 4:07:19 PM
To: Libby Gregoric <libby.gregoric@premiers.qld.gov.au>; Kristen Foster <kristen.foster@premiers.qld.gov.au>; Scott Mathewson <scott.mathewson@premiers.qld.gov.au>; Pamela Healy <pamela.healy@premiers.qld.gov.au>; Michael Phillips <Michael.Phillips@premiers.qld.gov.au>
Cc: Steven Wishart <steven.wishart@premiers.qld.gov.au>
Subject: RE: ESCALATION ADVICE - Queensland Government Cyber Security Arrangements

OFFICIAL

Hi Libby

We can confirm we are patched against both vulnerabilities mentioned below.

I'll advise further as information comes to hand.

Cheers

Leigh

Leigh Dixon
A/Director, Cyber Security *(she/her)*
Department of the Premier and Cabinet
T: 07 300 39416
E: Leigh.Dixon@premiers.qld.gov.au

Chat with me on Teams!

From: Libby Gregoric <libby.gregoric@premiers.qld.gov.au>
Sent: Wednesday, November 15, 2023 4:06 PM
To: Kristen Foster <kristen.foster@premiers.qld.gov.au>; Leigh Dixon <leigh.dixon@premiers.qld.gov.au>; Scott Mathewson <scott.mathewson@premiers.qld.gov.au>; Pamela Healy <pamela.healy@premiers.qld.gov.au>; Michael Phillips <Michael.Phillips@premiers.qld.gov.au>
Subject: Fwd: ESCALATION ADVICE - Queensland Government Cyber Security Arrangements

Fyi

Libby Gregoric
Deputy Director-General
People and Services
Department of the Premier and Cabinet
P: 07 3003 9046 M: Irrelevant
E: Libby.Gregoric@premiers.qld.gov.au

From: Libby Gregoric <libby.gregoric@premiers.qld.gov.au>
Sent: Wednesday, November 15, 2023 4:00:14 PM
To: Filly Morgan <filly.morgan@premiers.qld.gov.au>; Sally Lohrisch <sally.lohrisch@premiers.qld.gov.au>; Michelle Jackson-Hay <Michelle.Jackson-Hay@premiers.qld.gov.au>; Scott Mathewson <scott.mathewson@premiers.qld.gov.au>
Cc: Michael Phillips <Michael.Phillips@premiers.qld.gov.au>; Ella Bailey <ella.bailey@premiers.qld.gov.au>
Subject: Fwd: ESCALATION ADVICE - Queensland Government Cyber Security Arrangements

Libby Gregoric
Deputy Director-General
People and Services
Department of the Premier and Cabinet
P: 07 3003 9046 M: Irrelevant
E: Libby.Gregoric@premiers.qld.gov.au

From: SDCG Secretariat <Irrelevant>
Sent: Wednesday, November 15, 2023 3:41:33 PM
To: Kylie Mercer (IGEM) <kylie.mercer@igem.qld.gov.au>; Andrew Bryett <andrew.bryett@health.qld.gov.au>; Austin.PaulS[EM&CC] <Austin.PaulS@police.qld.gov.au>; belinda.drew <belinda.drew@chde.qld.gov.au>; Bosnjak.JohnM[EM&CC] <Bosnjak.JohnM@police.qld.gov.au>; Brendin Bloye <Brendin.Bloye@health.qld.gov.au>; Communities Email <Irrelevant>; CORRECTIONS DM BUSINESS EMAIL <Irrelevant>; Lisa Beach <lisa.beach@daf.qld.gov.au>; DAF BUSINESS EMAIL <Irrelevant>; DAF CORE Donaghy <Peter.Donaghy@daf.qld.gov.au>; DCHDE Proxy Andrew Spina <andrew.spina@hpw.qld.gov.au>; Arthur O'Brien (CYJMA) <arthur.o'brien@cyjma.qld.gov.au>; DCYJMA MGR DDG OFFICE

<jody.preston@cyjma.qld.gov.au>; DCYJMA PROXY - SHORT <Danny.Short@cyjma.qld.gov.au>; Dept of Resources EMC business account <Irrelevant>; graham.atkins <graham.atkins@epw.qld.gov.au>; DEPW ENERGY BEHNE <Paul.Behne@epw.qld.gov.au>; tara.gardiner <tara.gardiner@epw.qld.gov.au>; DEPW Proxy Scott Wilson <scott.wilson@epw.qld.gov.au>; DES CORE KIRTON <mike.kirton@des.qld.gov.au>; DES MCMAIN <lisa.mcmain@des.qld.gov.au>; DESBT - MAYER <Andrea.Mayer@desbt.qld.gov.au>; DESBT DISASTER SUPPORT BUSINESS <Irrelevant>; DESBT PROXY - LUCAS <david.lucas@desbt.qld.gov.au>; DJAG - IACUTONE <lisa.iacutone@justice.qld.gov.au>; DJAG CORE MUNRO <perry.munro@justice.qld.gov.au>; DOE CASEY <Chantal.CASEY@qed.qld.gov.au>; SHEEDY, Dave <Dave.SHEEDY@qed.qld.gov.au>; angela.stevens <angela.stevens@chde.qld.gov.au>; Donald W Bletchly <Donald.w.bletchly@tmr.qld.gov.au>; DOR - SORENSEN <leigh.sorensen@resources.qld.gov.au>; DOR CORE HARRYMAN <renee.harryman@resources.qld.gov.au>; Libby Gregoric <libby.gregoric@premiers.qld.gov.au>; Disaster Management <Irrelevant>; Scott Mathewson <scott.mathewson@premiers.qld.gov.au>; Tammy Woolf-Stefanutto <tammy.woolf-stefanutto@premiers.qld.gov.au>; Michelle Wellington (DPC) <michelle.wellington@premiers.qld.gov.au>; Emmy Kubainski <emmy.kubainski@premiers.qld.gov.au>; COWLEY-GRIMMOND Jarrod <jarrod.cowley-grimmond@rdmw.qld.gov.au>; DRDMW EMERGENCY CONTACT <Irrelevant>; Hamish.Butler <Hamish.Butler@rdmw.qld.gov.au>; DSDILGP - KELLY <Leah.Kelly@dsdilgp.qld.gov.au>; DSDILGP PROXY -HORTZ <tim.hortz@dsdilgp.qld.gov.au>; DSDILGP Vicki Battsglia <Vicki.Battaglia@dsdilgp.qld.gov.au>; Elissa Read (DSDSATSIP) <elissa.read@dsdsatsip.qld.gov.au>; Rhiannan Howell (DSDATSIP) <rhiannan.howell@dsdsatsip.qld.gov.au>; DTIS - COEHN <Kate.Coehn@dtis.qld.gov.au>; Sarah Vandersee <Sarah.Vandersee@dtis.qld.gov.au>; Adrienne J. Bailey <adrienne.j.bailey@tmr.qld.gov.au>; DTMR MARITIME <jim.a.HUGGETT@MSQ.QLD.GOV.AU>; DTMR MARITIME PROXY BEATTY <jonathan.j.beatty@tmr.qld.gov.au>; Enes Seferovic <enes.seferovic@qfes.qld.gov.au>; Glenn Alderton <glenn.alderton@qfes.qld.gov.au>; Glenn Miller <glenn.miller@treasury.qld.gov.au>; Graham.Rob[EM&CC] <Graham.RobJ@police.qld.gov.au>; Hamlett, Eloise <Eloise.Hamlett@Corrections.qld.gov.au>; HEALTH DM <Irrelevant>; Housing Proxy - O'Brien <james.o'brien@chde.qld.gov.au>; Lynn Snoddy (PSC) <lynn.snoddy@psc.qld.gov.au>; QAS CORE <Craig.Emery@ambulance.qld.gov.au>; QCS Core Joel Smith <joel.smith@corrections.qld.gov.au>; QCS Proxy - Lavin <Christopher.Lavin@corrections.qld.gov.au>; QRA POLICY <Irrelevant>; Rebecca Morris <rebecca.morris@qra.qld.gov.au>; Robin Boniwell <robin.boniwell@qfes.qld.gov.au>; Sally Lohrisch <sally.lohrisch@premiers.qld.gov.au>; Sandra Lerch <Sandra.Lerch@psc.qld.gov.au>; Shand.George[EM&CC] <Shand.George@police.qld.gov.au>; Stephen Zsombok <stephen.zsombok@ambulance.qld.gov.au>; Tina Girvan <tina.girvan@qra.qld.gov.au>; Jo Keen <Joanne.Keen@treasury.qld.gov.au>; Vina Varsani <Vina.Varsani@qra.qld.gov.au>

Cc: SDCG Secretariat <Irrelevant>; Danielle.Mahl <Danielle.Mahl@cyber.chde.qld.gov.au>

Subject: ESCALATION ADVICE - Queensland Government Cyber Security Arrangements

OFFICAL: SENSITIVE

Good Afternoon,

The Queensland Government Chief Information Security Officer has authorised an escalation of the Queensland Government Cyber Security Arrangements from **Level 5 (baseline)** to **Level 4 (Alert)**.

This decision is informed by the following considerations:

1. Sch 1 of the RTI Act - Security Document

1. [redacted]
2. Sch 1 of the RTI Act - Security Document

1. Some Australian States and Territories are tracking network scanning and other activity for these vulnerabilities.
2. The National Cyber Security Committee (NCSC) have unanimously authorised an escalation of the Cyber Incident Management Arrangements for Australian Governments from Level 5 to level 4.

This advice has been sent to Queensland Government departments, statutory bodies, councils, and government-owned corporations.

What the Queensland Government Cyber Security Unit (QGCSU) are doing in response:

1. The ACSC is working with the QGCSU to engage and request formal responses on all identified instances of exposure for Queensland Government entities.
    1. This engagement and the subsequent entity responses provide the ACSC and QGCSU with assurance that entities:
        1. Are aware of exposure.
        2. Have conducted investigations to determine if any of their systems have been compromised.
            1. detection of potential compromise prompts further incident response activity.
        1. Have applied appropriate mitigations (such as patching).
    1. The QGCSU will work with department cyber security leads and other stakeholder groups on specific entity/sector-based engagement if deemed required.
1. The NCSC's Operations Sub-Committee will be conducting daily meetings to update on response activity and arising needs/actions.
2. The Queensland Government Digital Leadership Group has been made aware of the activity, and Queensland Government cyber security leads are being convened by the QGCSU for an advisory brief tomorrow.

Unless new information prompts the need for an urgent update, a situation report on exposure and WoG response activity will be provided at 10:00 on Friday afternoon (17/11/2023).

1. Due to the sensitive nature of reporting content, the detailed WoG reporting will be provided to relevant QGCSU stakeholders only.
2. Outcomes from the QGCSU led advisory brief will be circulated to inform any independent briefing activity being conducted by Queensland Government entities.
    1. Further briefings will be arranged as necessary.
1. Future updates on this matter, including further escalation or de-escalation will be appropriately circulated by the QGCSU.

This advisory and email are marked OFFICIAL:SENSITIVE and TLP:AMBER. Please limit distribution to those employees with a strict "need to know" to inform any required briefings and the protection of your ICT systems. Recipients can share this material with ICT contractors.

Any queries relating to this matter may be directed to Rob Champion or Danielle Mahl via:

Irrelevant

Entities concerned about exposure or potential compromise through the above vulnerabilities should immediately report this to the CSU's Cyber Defence Centre via: Irrelevant.

Kind Regards,

Tracey Carroll
Acting Senior Sergeant
State Disaster Coordination Group Secretariat
Disaster Management Unit | Specialist Services Group | Queensland Police Service
Ph: 07 3635 3246 | **Mob:** Irrelevant | **Mail:** GPO Box 1440 Box Brisbane QLD 4000
Email: Irrelevant
Email: Carroll.TraceyL@police.qld.gov.au

OFFICAL: SENSITIVE

Irrelevant

From: Michelle Wellington (DPC)
Sent: Friday, 22 December 2023 12:50 PM
To: Premiers Media; Amy Hunter; Mike Kaiser; Emma Kinnane
Cc: Jessica Collins; Rebecca McGarrity; Crisis Communication
Subject: FW: WofG Talking Points - St Vincent's Health Australia cyber incident - V1 - 22 December 2023 [SEC=OFFICIAL]
Attachments: WofG Talking Points - St Vincent's Health Australia cyber incident - v1.docx

Hi Amy

Please find attached the latest Commonwealth talking points relating to the St Vincents cyber incident.

Kind regards,

Michelle Wellington (She/Her)
Assistant Director-General
Reform and Delivery
Chair, Crisis Communication Network
Department of the Premier and Cabinet

Queensland Government

M: Irrelevant
E: michelle.wellington@premiers.qld.gov.au
1 William Street, Brisbane QLD 4000
PO Box 15185, City East, QLD 4002

NB: I sometimes work and send correspondence out of hours. Please do not feel obliged to respond outside of your own work hours.

Queensland Good jobs Better services Great lifestyle

From: Crisis Media Operations <Irrelevant>
Sent: Friday, December 22, 2023 12:09 PM
To: Crisis Media Operations <Irrelevant>
Subject: WofG Talking Points - St Vincent's Health Australia cyber incident - V1 - 22 December 2023 [SEC=OFFICIAL]

OFFICIAL

Good afternoon all,

Please find attached version 1 of the Whole of Government talking points for the St Vincent's Health Australia (SVHA) cyber incident.

A statement from St Vincent's is available here. Following this, a statement has also been issued on the National Cyber Security Coordinator channels.

These talking points will be updated and reissued as required.

If your agency wishes to provide input/changes, please send them with tracked changes in the document to Irrelevant

Kind regards,

Hayley

National Security and Crisis Communication
Department of Home Affairs
Crisis media on-call: M Irrelevant | E: Irrelevant

OFFICIAL

Australian Government

Department of Home Affairs

TALKING POINTS

Subject	St Vincent's cyber incident	
Date	22 December 2023	**Version 1**
Type	Whole of Government	
Media Officer: Tracy Heffernan		**Media Ph:** 02 6264 2244

ISSUE

Cyber incident impacting St Vincent's Health Australia

TALKING POINTS

- St Vincent's Health Australia is the victim of a cyber incident impacting their networks and data.
    - St Vincent's is a not-for-profit health and aged care provider, offering services in Queensland, New South Wales and Victoria, including public and private hospitals and aged care facilities.
- We know cyber incidents can be distressing for those affected.
- The Australian Government is working with states and territories to support St Vincent's with a nationally coordinated response to this incident.
- The Acting National Cyber Security Coordinator is receiving regular briefings.
    - We are focused on assisting St Vincent's to consider and address impacts arising from this incident.
- St Vincent's has taken immediate steps to contain the incident and is prioritising the health and safety of its patients and people and the continuity of services for the community.
- St Vincent's has advised that this incident has not affected their ability to deliver their important services to patients, residents, and the broader community across their hospital, aged care, and virtual and home health networks.
- The Australian Signals Directorate's Australian Cyber Security Centre (ACSC) has offered technical advice and assistance.
- St Vincent's has contacted the Office of the Australian Information Commissioner about the incident.
- Work to resolve this incident is ongoing.
    - St Vincent's has advised that it first notified the ACSC and state regulators on 19 December, the day that they became aware of the incident.

- Specific enquiries relating to this incident should be directed to St Vincent's.

CLEARANCE

Drafted by	Title	Time/Date drafted
Tracy Heffernan	Director, National Security and Crisis Communication	22 December 2023
Consultation	Services Australia, Health, Digital Health, OAIC, ASD	22 December 2023

Cleared by	Title	Time/Date cleared
Hamish Hansford	A/g Cyber Security Coordinator	22 December 2023
Tracy Heffernan	Director, National Security and Crisis Communication	22 December 2023

Irrelevant

From: Mike Kaiser
Sent: Monday, 8 January 2024 9:48 AM
To: ECU Correspondence
Subject: FW: Correspondence from the Under Treasurer of Queensland - Our Ref 04812-2023
Attachments: Correspondence from Under Treasurer - Our Ref 04812-2023.pdf

Importance: High

Hi ECU

For registration and allocation thank you

Regards
Emma

From: Executive Correspondence <Irrelevant>
Sent: Friday, January 5, 2024 4:02 PM
To: kylie.rampa@qic.com
Cc: Mike Kaiser <mike.kaiser@premiers.qld.gov.au>; robert.champion@cyber.chde.qld.gov.au
Subject: Correspondence from the Under Treasurer of Queensland - Our Ref 04812-2023
Importance: High

You don't often get email from Irrelevant. Learn why this is important

OFFICIAL

Dear Ms Rampa

Please find attached correspondence from the Under Treasurer of Queensland.

Kind regards

Executive Correspondence
Queensland Treasury
Web: www.treasury.qld.gov.au

QUEENSLAND TREASURY

www.treasury.qld.gov.au

Queensland Government

Queensland Treasury

Our Ref: 04812-2023

Ms Kylie Rampa
Chief Executive Officer
QIC Limited
GPO Box 2242
BRISBANE QLD 4001

Email: kylie.rampa@qic.com
Cc: mike.kaiser@premiers.qld.gov.au
robert.champion@cyber.chde.qld.gov.au

Dear Ms Rampa

As you are aware, Queensland's government-owned corporations (GOC) and commercial statutory authorities (Seqwater and Queensland Rail) provide essential energy, water, transport and trade services which are vital to the Queensland economy. It is therefore important that government has confidence in the ICT systems that control the operation of these entities and their critical assets.

Recent events highlight the very real threat that cyber security attacks pose to critical service providers and the potential for these attacks to cause significant disruption to the economy and community at a local, state and national level.

I am writing to reiterate the importance the Queensland Government places on best-practice cyber security risk management. The previous GOC cyber security review, completed in late 2022, highlighted the need to increase investment in cyber security capability uplift. I thank you for your continued efforts in actioning recommendations from this review.

Recent amendments to the Australian *Security of Critical Infrastructure Act 2018* (SOCI Act) have imposed additional requirements upon providers of essential and critical services, which captures all government-owned energy, water and transport businesses. GOCs will need to have a compliant cyber security framework by 17 August 2024 and meet mandatory reporting requirements on critical infrastructure, risk management plans and cyber security incidents.

The Queensland Government is committed to ensuring compliance with this legislation. Queensland Treasury, along with the Queensland Government's Chief Information Security Officer and the Cyber Security Unit, will continue to work closely with GOCs regarding cyber security and the SOCI Act.

1 William Street
GPO Box 611 Brisbane
Queensland 4001 Australia
Telephone +61 7 3035 1933
Website www.treasury.qld.gov.au
ABN 90 856 020 239

This will include a follow-up cyber security review in early 2024. The review will consider how entities are tracking towards meeting requirements under the SOCI Act and their cyber security capability. Queensland Treasury will keep you informed as the scope and terms of reference are developed.

If you have not already, I request you engage with the Queensland Government Cyber Security Unit (QGCSU) and take advantage of the centrally funded cyber security services available to all Queensland Government Statutory entities. For more information, please contact Ms Sarah Brown of the QGCSU Engagement Team, Queensland Government Customer and Digital Group – Department of Transport and Main Roads, on Irrelevant by email at Irrelevant or by visiting www.forgov.qld.gov.au/information-and-communication-technology/cyber-security/about-the-cyber-security-unit.

It is expected that Queensland Government entities report all cyber security incidents to the QGCSU on (07) 3215 3951 and at Irrelevant This reporting builds a picture of the threats we face and can provide you with specialist assistance and advice during a cyber incident. Details on this service can be found at www.forgov.qld.gov.au/information-and-communication-technology/cyber-security/report-a-cyber-security-incident.

If you require any further information, please contact Mr Grant Gaston, Acting Assistant Under Treasurer, Government-Owned Corporations Performance and Governance, Queensland Treasury, on Irrelevant, who will be pleased to assist.

Yours sincerely

Irrelevant

Michael Carey
Under Treasurer

22 / 12 / 2023