Australian Government
Office of the Australian Information Commissioner

Data Breach Response Team - Meeting Minutes

Date:	23 June 2022
Time:	3.00pm
Dial-In (TEAMS):	Microsoft Teams meeting **Join on your computer or mobile app** Click here to join the meeting **Join with a video conferencing device** 839060488@t.plcm.vc Video Conference ID: 137 636 980 2 Alternate VTC instructions **Or call in (audio only)** +61 2 7208 4918,,150955430# Australia, Sydney Phone Conference ID: 150 955 430#
Conference ID:	137 636 980 2
Present:	Caren Whip (Chair), s. 22
Apologies	s. 22
Observers:	Nil

For Decision and Executive Briefs

Background

On 23 June 2022, Caren Whip, General Counsel and Chief Privacy Officer convened the Data Breach Response Team (**response team**) to test the Office of the Australian Information Commissioner's (**OAIC**) Data Breach Response Plan (**DBRP**).

1. CW advised the response team that the meeting was convened due to an alleged data breach.
2. CW provided an overview of the requirement to test the OAIC Data Breach Response Plan as part of the compliance activities under the OAIC Privacy Management Plan (D2021/015576).

3. The response team reviewed the data breach scenario emails from the OAIC officer and Director involved. The scenario involved an OAIC officer inadvertently sending a list of privacy matters under current investigation to their Gmail account in an attempt to print the list from their home printer, while working from home. The matter was referred to the Director and the Director advised the Chief Privacy Officer (CPO). A message was sent to journalist asking for the deletion of the email but the officer had not yet heard back.

4. CW sought advice and suggestions from response team as to what next steps could be taken.

5. The response team referred to the checklist contained in the Data Breach Response Plan (D2022/013014).

6. s. 22 suggested drafting a media statement and alerting all staff.

7. s. 22 noted that it may be useful to include notification to Strategic Communications early on to consider whether it was necessary to issue a media release or statement, and/or notify OAIC staff.

8. CW noted that the Data Breach Response Plan makes some reference to the media action to be taken where there is there possibility of the breach resulting in media attention/reputational risk to the OAIC/the Commissioner.

   ACTION ITEM 1: *Review Data Breach Response Plan and consider updating checklist to more specifically include notification to Strategic Communications. Note – the Data Breach Response Plan refers to a list of considerations, including communications or media strategy to manage public expectations and media interest (page 11).*

9. CW noted that the recommendation to notify OAIC staff was a useful one, and could be using as a whole of office learning.

10. s. 22 suggested phone call to the journalist and affected individuals. There was no information regarding number of affected individuals.

11. Response team discussed additional details such as number of complainants and further details would be useful.

12. CW noted that usually there would be more information sought prior to convening the meeting and proposed inviting the Director who was notified of the breach to be present in the response team meeting.

    ACTION ITEM 2: *Consider amending the Data Breach Response Plan to include involving relevant Director to be part of the initial response team meeting to provide context or additional information to help inform response team determine appropriate next steps.*

13. s. 22 raised the need to consider whether the possibility of circulation of information about the breach would compound potential harm and raised question of whether respondent was identified.

14. CW noted primary action would be to notify journalist to see if they would be agreeable to deleting the document or whether they sought to use the information contained in the document. Response team would need to have a plan A and B to account for both scenarios.

15. CW advised that if this was an actual data breach, attempts would be made to contact the journalist and the Executive would be put on notice. The response team would be convened as a matter of urgency rather than be given the 2-3 hour notice before the meeting, as was the case for this simulation.

16. The response team discussed how affected individuals should be notified. FA suggested it was the list was short, individuals should be called and notified. If it was a longer list then perhaps an email then a follow up phone call.

17. Response team noted that while complaint file number may not be an issue, name and due date may potentially be detrimental to some people, depending on the nature and circumstances of their complaint, e.g. domestic violence situation.

18. CW noted that a number of useful suggestions have been made and that minutes will be circulated to the response team for consideration.

19. CW asked the response team to let her or s. 22 know if they have any additional thoughts or suggestions following the conclusion of the meeting.

ACTION ITEM 3: *Response team to consider whether there are any additional steps or considerations that need to be taken for simulated data breach or in terms of amendments to the Data Breach Response Plan.*

Action Items

1. To review the Data Breach Response Plan to include consultation with Strategic Communications
2. To review the Data Breach Response Plan to include reporting Director to attend response team meeting
3. Response team to consider providing any additional comments or suggestions regarding the data breach simulation exercise or Data Breach Response Plan amendments.

#	Description	Delegate	Due Date	Status	Notes
	1. To review the Data Breach Response Plan to include consultation with Strategic Communications	Caren Whip, Chief Privacy Officer	30 June 2023		To be considered as part of the regular review of the OAIC Data Breach Response Plan under the Controlled Documents Framework.
	2. To review the Data Breach Response Plan to include reporting Director to attend response team meeting	Caren Whip, Chief Privacy Officer	30 June 2023		To be considered as part of the regular review of the OAIC Data Breach Response Plan under the Controlled Documents Framework and OAIC Privacy Management Plan.
	3. Response team to provide further feedback	Data Breach Response Team	27 June 2022		Please respond with any suggestions by COB Monday 4 July 2022.

Australian Government
Office of the Australian Information Commissioner

Memorandum

To	Senior Assistant Commissioner, Privacy Champion
From	s. 22 Lawyer
Copies	Chief Privacy Officer
File ref	LEG22/00082
Date	21 June 2022
Subject	**Data Breach Response Simulation Test 2022**

On 23 June 2022, Caren Whip, General Counsel convened the Data Breach Response Team (**response team**) to test the Office of the Australian Information Commissioner's (**OAIC**) Data Breach Response Plan (**DBRP**).

Privacy Management Plan Compliance Activity

The Privacy Management Plan FY 22 requires that the OAIC conduct an annual data breach simulation test to ensure that its Data Breach Response Plan remains effective, current and relevant. In preparation for the simulation:

1. The response team primary contact list was updated to ensure that information was current and members can be easily contacted by staff, and each other, to facilitate a timely response to actual or suspected data breach incidents.
2. A secondary contact was provided to ensure that there are sufficient people who can respond if key personnel are unavailable due to illness or other factors.
3. A scenario involving a working from home related incident was identified on which to base the simulation.

The simulation exercise was carried out on 23 June 2022.

Recommendations

1. Note that the DBRP has been tested through simulation exercise.
2. Note that the DBRP will be reviewed in FY 23 to incorporate feedback from the response team.

3. Note the data breach simulation test as completed for the purposes of the Privacy Management Plan FY 22.

Data Breach

The test scenario and related material is set out at Annexure A.

The Response Team treated the test as if it were an actual incident. The Response Team went through the steps set out in the DBRP and all steps were satisfied.

The simulation did identify some amendments that could be made to the Data Breach Response Plan to improve its effectiveness and comprehensiveness. Those actions are outlined in the Minutes to the Breach Response Team Meeting (Simulation Exercise), and will be undertaken in Q1 of FY23.

Data Breach Response Team convened

The Data Breach Response Team (**response team**) was convened at 3:00 pm 23 June 2022 to test the Office of the Australian Information Commissioner's (**OAIC**) Data Breach Response Plan (**DBRP**).

Each team across the OAIC was represented as follows:

Team	Representative
Legal Services	s. 22
Regulation & Strategy	s. 22
Privacy Dispute Resolution	s. 22
Strategic Communications	s. 22
FOI Regulatory Group	s. 22

Meeting minutes can be viewed via Content Manager: D2022/014082

Data Breach Response Plan

Response Team consideration/assessment

Step 1: Identify the breach (OAIC officer)

- ☐ Record and advise your Director of the following:
  - the time and date the suspected breach was discovered,
  - the type of personal information involved,
  - the cause and extent of the breach, and
  - the context of the affected information and the breach.

There is evidence (Officer's email) that the officer notified the Director in a timely manner. It was noted that more information could be provided regarding the extent of the breach and types of personal information involved. CPO noted that usually further enquiries would have been made prior to convening the meeting and suggested the including the reporting Director in the response team meeting as a step to allow the response team the opportunity to clarify any questions to help inform options for next steps.

This step has been satisfied.

Step 2: Contain the breach (EL2 Director)

- ☐ Understand and assess the data breach, or suspected data breach
- ☐ Co-ordinate any action required to contain the data breach
- ☐ Notify the Chief Privacy Officer about the data breach.

There is evidence (the email from the Director to the officer and to the Chief Privacy Officer (CPO)) that the Director assessed the breach and directed the officer to contact the third party to request the deletion of the email. The Director could have provided the CPO with an assessment of the likely impact the incident may have on the affected individuals and advise whether notifying individuals would be appropriate. The Director then notified the CPO as appropriate.

Note: As this was a test scenario, actions of the Officer and Director have been hypothetical and as such, does not necessarily represent whether appropriate training is required. However, it may be useful to send a reminder to OAIC staff of their obligations under the DBRP.

This step has been satisfied.

Step 3: Assess the risks for individuals associated with the breach (Chief Privacy Officer)

- ☐ Conduct initial investigation to establish the cause and extent of the breach.
- ☐ Assess priorities and risks based on what is known.
- ☐ Notify OAIC Executive about the data breach.
- ☐ Keep appropriate records of the suspected breach including any action taken.

CPO noted that she would usually make further enquiries and put the Executive on notice prior to convening the meeting given the nature of the breach. Data breach incident emails are kept in Content Manager and recorded in the Data Breach Incidents log.

This step has been satisfied.

Step 4: Consider breach notification and convene response team

- ☐ Determine who needs to be made aware of the breach at this preliminary stage.
- ☐ Determine whether and how to notify affected individuals.
- ☐ Determine whether to escalate the data breach to the response team.
- ☐ Convene the response team, if necessary.
- ☐ Determine whether the breach is an eligible data breach under the NDB scheme.
- ☐ Notify the AIC of the NDB, if necessary.

CPO determined the Executive, Strategic Communications and Data Breach Response Team needed to be made aware at the preliminary stage. The Data Breach Response Team was convened.

The response team discussed:

- *Individual should not have sent work to personal email account*
- *possible methods of notification to affected individuals via releasing a Statement, email and phone calls.*
- *the CPO noted that she would have put Executive on notice about the response team being convened*
- *a report of the meeting would be provided to the AIC regarding the NDB. Minutes were drafted and provided to CPO on the same day for circulation to response team and Executive for consideration.*
- *First step is to identify further information regarding the privacy complaints list or document at issue and to contact the third party (journalist) to confirm whether the email was deleted or intentions otherwise.*
- *Second step would be to notify Executive, Strategic Communications and convene the Data Breach Response Team immediately.*
- *The next step would be identifying the best way to notify affected individuals, OAIC staff and issuing a statement as appropriate.*

This step has been satisfied.

Step 5: Review the incident and take action to prevent future breaches

- ☐ Fully investigate the cause of the breach.
- ☐ Implement a strategy to identify and address any weaknesses in OAIC data handling.
- ☐ Conduct a post-breach review and report to OAIC Executive on outcomes and recommendations.

To fully investigate the cause of the breach additional information is required from the officer and Director. The CPO hypothetically investigated the breach and noted in this incident that the determined the Executive, Strategic Communications and Data Breach Response Team needed to be made.

In order to ensure the response team has adequate information to inform appropriate next steps, it was proposed that the reporting Director be included in future Data Breach Response Team meetings convened where appropriate.

It was identified that further investigation should be made as to strategies that could be in place to prevent the incident from reoccuring? Eg, did it occur due to the officer not disabling the Auto Fill function in Outlook?

The response team noted further consideration were necessary to determine whether the notification to affected individuals, public statements and/or OAIC Staff would cause more harm was discussed.

Recommendations arising from the exercise include

- Reviewing the DBRP checklist to include notification to Strategic Communications where appropriate and do so
- Including the possibility of inviting reporting Director to response team meetings convened following an alleged data breach
- Reviewing the DBRP in consultation with the response team generally for additional feedback.

This step has been satisfied.

Annexure A

Data breach

Dear Director,

My apologies, I think I may have committed a data breach.

I have inadvertently sent a list of privacy matters being investigated to a journalist this morning at 9.35am.

I wanted to print the list of privacy matters and intended to send it to my personal Gmail account so that I may print the document at home given that I did not have access to the office printer while working from home.

I noticed it did not go to my Gmail account after a few minutes of waiting and when I checked the email in my Outlook 'sent' folder, I realised the email did not go to my Gmail, rather it went to a journalist.

The list of current privacy matters that are being investigated contains open case file numbers, complainant names and due dates.

Please advise what actions I need to take.

Thanks,

OAIC officer

Thanks OAIC Officer,

Please request that the third party delete the information and seek confirmation of this in writing. I will advise the Chief Privacy Officer of the breach.

Regards,

Director

Dear Chief Privacy Officer,

I am notifying you of a data breach that occurred yesterday. Please see the emails from my staff member this morning at 9.35am. A list of current privacy matters being investigated was inadvertently sent to a journalist.

I have requested the staff member to contact the third party and seek confirmation that the email was deleted. We are still waiting for confirmation.

Please advise if there is any further information you would like me to provide.

Regards,

Director

Senior Assistant Commissioner Notification

From: Caren Whip
Sent: Thursday, 21 June 2022 2:33 PM
To: Acting Deputy Commissioner
Cc:
Subject: [Test] Executive notification of data breach [SEC=OFFICIAL]
Attachments: Urgent: Data breach [SEC=OFFICIAL]
Security Classification:

OFFICIAL

Dear Acting Deputy Commissioner,

**** this is a test simulation****

We ran a data breach simulation and tested the Data Brach Response Plan on Thursday, 23 June 2022. I was able to convene the data breach response team within 2.5 hours to discuss the outcome of data breach scenario.

The memo outlining the hypothetical scenario and outcome is attached.

If you have any questions please let me know.

Regards,

Caren Whip
General Counsel
[sig block]