Fact Sheet December 2023

How to calculate the estimated cost of a data breach

Who is this information for?	NSW public sector agencies seeking information on calculating the cost of a data breach
Why is this information important to them?	This fact sheet will assist agencies to estimate the cost of a data breach for the purpose of notification under the MNDB Scheme

When a public sector agency notifies the Privacy Commissioner of an eligible data breach under the Mandatory Notification of Data Breach Scheme (MNDB Scheme), the agency must include information on the estimated cost of the data breach[1].

This fact sheet provides guidance on the matters that an agency should consider when estimating the costs of a data breach and the items that should be included in the estimate.

Costs arising from containment and assessment activities

Agencies should include any costs incurred during the assessment of a data breach or while attempting to contain a data breach. This may include:

Actions taken to contain a data breach

Any action that an agency takes to stop or limit any further access, disclosure or loss of personal information, or actions to retrieve personal information that has already been exposed by a data breach.

This may include:

- actions to recover or limit the dissemination of personal information disclosed without permission.
- security upgrades to systems or databases.
- shutting down a compromised system.
- recovery of lost devices or hard copy records, or
- remote deletion of personal information from lost or stolen devices.

Assessment activities

Any costs associated with conducting a data breach assessment including:

- appointment of an assessor – this can be a staff member or an external consultant
- investigation activities undertaken to confirm whether a data breach has occurred or to determine the nature and extent of the breach
- forensic investigations or audits of systems to identify the specific information affected by the breach, or individuals affected by the breach, and
- legal advice sought in relation to the assessment process.

Agencies should estimate the costs of these activities whether undertaken by staff or officers of the agency or by specialist contractors engaged specifically for the assessment process.

Actions taken to mitigate harm

Agencies should estimate the costs of any actions taken to mitigate the harm to affected individuals. Mitigation strategies adopted will vary depending on the type and nature of the breach, and the potential harm to individuals the breach may cause.

Costs arising from making notifications

Agencies should include any costs incurred when making notifications to affected individuals.

This may include:

Sending notifications to affected individuals

The cost for the preparation and dispatch of notifications to affected individuals. This could include emails, letters, and phones calls.

[1] Section 59M(2)(g), PPIP Act 1998

Issuing a public notification

The cost for preparing and publishing a public notification on the agency's website.

Agencies are required to take all reasonable steps to publicise a public notification. Any costs incurred in publicising the notification should be included in the estimate of costs.

Providing assistance to affected individuals

Agencies should include the costs associated with providing advice or assistance to affected individuals.

- This may include:
- a dedicated help desk and inbound communications supports
- credit monitoring and identity protection services
- issuing new accounts or credentials
- referrals to other services, and
- contracts with third party service providers.

Costs arising from post-breach review activities

Following a data breach, agencies are encouraged to undertake a post-breach review to assess the effectiveness of the data breach policy and breach response. These costs should be considered as part of the estimate of costs.

This may include costs related to:

- reviewing and updating the agency's data breach plan
- reviewing and updating the agency's data breach response, including any changes to policies, systems, processes or procedures, or
- any legal advice sought in relation to the post-breach review.

Costs arising from the exercise of review rights

Individuals affected by a data breach may seek to exercise their review rights under the *Privacy and Personal Information Protection Act 1998* (PPIP Act) following notification. Costs likely to be incurred by the agency as a result of individuals exercising these rights should be included. This may include:

- costs associated with conducting internal reviews
- cost associated with proceedings in the NCAT, including internal staff costs, any external legal representation and any damages awarded by the Tribunal, or
- any ex-gratia payments made to affected individuals.

It is acknowledged that agencies are unlikely to have sufficient information to estimate these costs at the time of the initial notification to the Privacy Commissioner.

Once notification to individuals has occurred, agencies may be able to estimate potential costs arising from exercise of review rights, for example by extrapolating from internal review requests received in a particular period post-notification. This information can then be provided in a follow-up notification under section 59Q of the PPIP Act.

Are there any costs that should not be included?

The estimate of costs should only include those costs which have been or will be incurred by the agency because of the data breach.

Any routine costs that the agency would already incur as part of its usual course of business should not be included when estimating the cost of a data breach. This may include:

- regularly scheduled cybersecurity activities
- routine maintenance on agency information management systems, databases or customer relationship management systems
- regular testing of data breach response plans;
- regular reviews of systems, policies and procedures for the handling of personal information, and
- regular or ad hoc security up grades or patch updates, except where these occur as a direct result of a data breach.

What if the agency doesn't know the estimated costs at the time of notification?

Notification must be made to the Privacy Commissioner **immediately** after the head of the agency determines that an eligible data breach has occurred or is likely to have occurred.

The MNDB Scheme recognises that an agency may not be in a position to provide all of the information required for a notification at this point in time. Agencies may omit information from their notification to the Privacy Commissioner if it is not reasonably practicable to provide it.

Agencies must provide a follow-up notification to the Privacy Commissioner of any information that was not included in the original notification.

Other Matters to Consider

The estimate of costs should be assessed by considering the actual or anticipated costs incurred by the agency when responding to that specific data breach.

Agencies should not rely on costs incurred from previous breaches or published research analysing the average cost of a data breach.

Record keeping

Agencies should ensure that appropriate records are maintained of any information from which the estimate of the costs is derived.

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au

NOTE: The information in this fact sheet is to be used as a guide only. Legal advice should be sought in relation to individual circumstances.