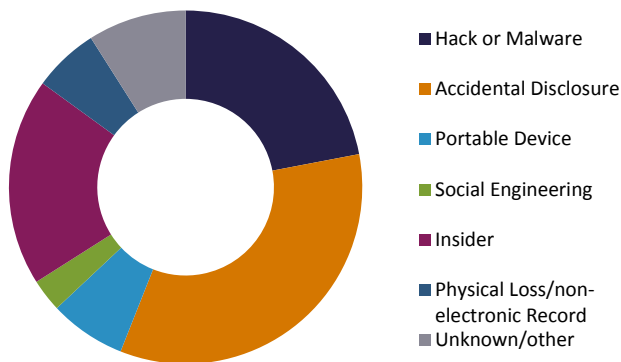


IF YOU HAVE DATA, YOU HAVE RISK. NEW DATA BREACH LEGISLATION AND HOW IT COULD IMPACT YOU

The risk of cyber attacks on Australian businesses is considered “High”. Recent data also shows that Healthcare professionals and organisations continue to be one of the most targeted.

Healthcare Incidents - Q4, 2017



As of February 2018, it is mandatory for businesses to notify of any data breach, and this must be done within 30 days to avoid a penalty. Last year, less than half of the documented cyber breaches were self-reported.

Who does this apply to?

This legislation is focused on businesses earning more than \$3M annually, however the new law applies to all Australian businesses storing potentially harmful data.

What is a notifiable breach?

The Office of the Australian Information Commissioner (OAIC) advises that a breach is notifiable where the following 3 criteria are met:

- 1. Unauthorised Access**
There is unauthorised access to, disclosure or loss of personal information that you hold.
- 2. Harmful Data**
This is likely to result in serious harm to one or more individuals.
- 3. No Prevention**
The likely risk of serious harm has not been prevented with remedial action.

You Experience a Data Breach. Now What?

1. Confirm the risk of serious harm

While “Serious Harm” is not defined in the Privacy Act it may include physical, psychological, emotional, financial or reputational harm.

The OAIC advises a broad approach should be taken when assessing the likelihood of harm, and to evaluate a number of key factors:

- The type & sensitivity of data
- Protection measures
- Likelihood of a data breach
- Nature of the harm

Having assessed that the data breach is likely to result in “serious harm” and remedial action is either not possible or unsuccessful you must notify affected individuals and prepare a statement for the Australian Information Commissioner.

2. Notifying Individuals

There are 3 options for notification:

Method	To Consider	Requirements
Notify all affected individuals	You may not have up-to-date contact details for all individuals involved.	N/A
Only notify individuals at risk of “serious harm”	Avoid any unnecessary alarm to individuals who aren’t affected. However, individuals who were affected could be missed.	N/A
Publish Notification	Could help notify affected individuals if you don’t have current contact information.	A copy of the statement must be published on your website (if one exists)

3. Notify the Australian Information Commissioner

You will need to prepare a Notifiable Data Breach (NDB) Statement from the OAIC website which will need to include:

- Your business's identity and contact details
- A description of the eligible data breach
- Kind(s) of information involved in the data breach
- The steps you recommended individuals take in response to the data breach

Not sure how to structure your statement?

The OAIC provides access to an online form allowing the ability for you to notify of a data breach online. You can access this online form at:

Additional OAIC resources available

[Click here](#) to access the OAIC online NDB Statement

[Click here](#) for a guide to managing data breaches

[Click here](#) for a guide to securing personal information

[Click here](#) for a webinar on preparing your business for the NDB scheme

[Click here](#) for information on notifying individuals

[Click here](#) for information on what to include in an NDB statement

[Click here](#) for a data breach response summary

[Click here](#) to view the 2017 ACSC Threat Report



Cyber Security & Privacy Liability Insurance

The DHAA Insurance Program provides members exclusive access to leading Cyber coverage.

Premiums start at \$300 for limits up to \$1M.

This product covers you for:

- Notification costs, identity restoration services, and credit monitoring for the individuals whose information was compromised;
- The costs to engage a computer expert with the technical know-how required to identify the source of the data breach and protect against future incidents;
- The costs to hire a public relations firm to repair any damage done to your organization's reputation or image as a result of the breach;
- Fees associated with a regulatory investigation, including your legal defence, any fines and penalties the organization is required to pay (as permitted by law), and compensation for individuals who have been affected by the breach.

Call a specialist broker today to discuss your individual circumstance and ensure you're adequately covered.

DHAA & BMS are *Your Partners in Protection*.

If you have any questions relating to coverage or the DHAA Member Insurance Program, contact BMS on 1800-940-762 or email dhaa@bmsgroup.com.

This article contains general information, does not take into account your individual objectives, financial situation or needs. For full details of the terms, conditions and limitations of the covers, refer to the specific policy wordings and/or Product Disclosure Statements available from BMS Risk Solutions Pty Ltd on request. BMS Risk Solutions Pty Ltd arranges the insurance and is not the insurer.