Australian Privacy Amendment (Notifiable Data Breaches) Bill 2016

Business Brief

Cylance® Can Help

- Learn more about how we help our customers prevent breaches every day.
- The best **cybersecurity defence** is a great offense. CylancePROTECT® prevents threats and malware before they can execute.
- Full visibility and reporting is the best kind of visibility. Learn more about CylanceOPTICS™, an EDR solution that builds upon the superior threat prevention capabilities of CylancePROTECT.
- Concerned you've already been compromised? Or just want a full analysis of your environment and the potential weaknesses in your security strategy? Schedule a Compromise Assessment.

What It Is

The Privacy Amendment (Notifiable Data Breaches) Bill 2016 was passed by the Australian Federal Government on February 13, 2017, and is now awaiting Royal Assent.

The policies outlined within the bill are expected to be officially enacted within 12 months of its passing, and all Australian organisations, organisations that carry on business in Australia, or those otherwise bound by the Privacy Act, should proactively prepare to comply with the bill when it becomes active law.

Once the bill's policies are enacted, all organisations impacted by the new legislation will be legally required to report any 'eligible data breaches' to the Australian Privacy and Information Commissioner, and to notify customers who have been – or may have been – affected as soon as possible.

For the purposes of this bill, the term 'eligible data breach' is defined as any data breach where "*unauthorised access to or disclosure of information occurs and that access or disclosure would be likely to result in serious harm to any of the individuals to whom that information relates, or information is lost in circumstances where such unauthorised access or disclosure is likely to occur and, assuming such access or disclosure did occur, it would be likely to result in serious harm to any of the individuals to whom that information relates.*"

Who Is Affected

The Australian Privacy Amendment Bill applies to **all Australian government agencies, businesses, and not-for-profit organisations governed by the Privacy Act** with an annual turnover of more than $3 million, with some exceptions.

It is important to note that some small business operators (organisations with a turnover of $3 million or less) are also covered by the Privacy Act, including:

- **Private sector health service providers**, such as organisations like traditional health service providers (private hospitals, day surgeries, medical practitioners, pharmacists, and allied health professionals), complementary therapists (naturopaths and chiropractors), gyms and weight-loss clinics, or child care centres, private schools, and private tertiary educational institutions.
- **Businesses and individuals that handle**, use, and manage personal information, such as consumer credit information, credit reports, and tax file numbers.

About Cylance

Cylance is the first company to apply artificial intelligence, algorithmic science and machine learning to cybersecurity and improve the way companies, governments and end-users proactively solve the world's most difficult security problems. Using a breakthrough predictive analysis process, Cylance quickly and accurately identifies what is safe and what is a threat, not just what is in a blacklist or whitelist.

By coupling sophisticated machine learning and artificial intelligence with a unique understanding of an attacker's mentality, Cylance provides the technology and services to be truly predictive and preventive against advanced threats.

Why This Matters

In order to comply with these requirements, the impacted organisations must ensure they have the capabilities to:

- Determine whether an eligible data breach has occurred within 30 days of developing a suspicion of such a breach
- Prepare a report that outlines the relevant contact details, nature of the breach, and recommended steps for affected individuals to take in response
- Notify affected and at-risk individuals of the report contents as soon as possible, and if direct notification is not possible, publish the report on the organisation's website and publicise its contents

Any organisation that fails to comply with the new legislation may experience the following consequences:

- Risk of paying compensation (and court proceedings by the OAIC for the payment of compensation if the organisation fails to comply)
- Risk of paying civil penalties of an amount up to $1.8 million, in the case of corporations

Recommended Actions

In preparation for compliance with the new legislation, every organisation should:

- Strengthen and optimize its **cybersecurity strategy, technology, and overall defences**
- Ensure that steps are in place to **prevent a data breach**
- Review **data collection, handling, and breach practices and policies**
- Audit **data storage practices and locations** (i.e. with third parties or in the cloud) to ensure personal information is collected and stored only when needed
- Ensure it can supply the **visibility and reporting required**

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

©2017 Cylance Inc. Cylance® and CylancePROTECT® and all associated logos and designs are trademarks or registered trademarks of Cylance Inc. All other registered trademarks or trademarks are property of their respective owners.

20170502-1000