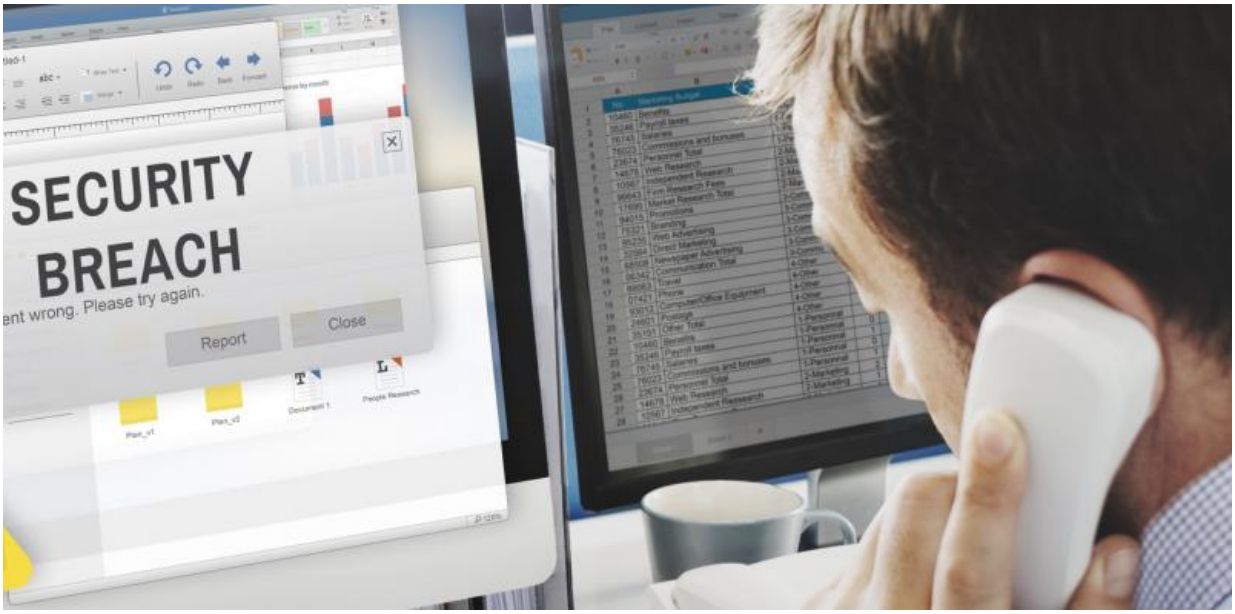
New law will force some (but not all) organisations to reveal data breaches

March 10 2017, by Jai Galliott



Changes to the way some organisations must reveal a data breach on personal information. Credit: Rawpixel com

We live in an era of big data stored digitally, and some of that data is about you. For example, the government keeps your social security and tax data, banks keep your financial data and your phone provider stores your metadata.

There is probably more of your confidential information in the data

storage facilities of various organisations than you have in your own filing cabinet.

But these organisations cannot always exercise control over it.

This will become ever more true as the reach of social media technologies increases. More and more of your photos, videos and personal dating stories will be converted into vulnerable bits and bytes.

Security breaches

All of this increases the risks associated with security breaches. Others might steal your information and use it for purposes for which it was not intended, such as fraud and intimidation.

Having identified this risk, the Australian Legal Reform Commission (ALRC) convinced the government that it would be beneficial to impose a notification requirement on organisations that could suffer data breaches.

If your personal information was compromised by a breach, this would allow you to take remedial steps to lessen the adverse impact.

This might range from a simple password change, to telling your spouse, family or employer about financial troubles, health conditions or secret memberships with Tinder, Grindr or Ashley Madison.

The Privacy Amendment (Notifiable Data Breaches) Bill 2016 has therefore quietly passed through parliament. It only needs Royal assent before the relevant legislation is enacted.

But will it do any good in the war on cybercrime?

Will it work?

This Bill is certainly a step in the right direction. It implements the ALRC recommendations by requiring organisations regulated by the Privacy Act to provide notice to the Australian Information Commissioner and affected individuals of an eligible data breach.

This provides both individuals and government with an opportunity to track and respond to events provided they pose a "a likely risk of serious harm" – whether this is financial, psychological, technological or otherwise.

It could be a malicious breach of the secure storage and handling of information, an accidental loss (most commonly of IT equipment or hard copy documents) or a negligent or improper disclosure of information.

But there are several problems that limit the legislations's effectiveness. To begin with, the means of notification are rather vague and leave much to be desired.

For instance, Section 26WL permits those reporting harmful breaches to use whatever communication method is regularly used with particular individuals, likely email.

But there is no regard for the fact that these regular means of communication are those most likely at risk. The most vulnerable people are typically those who don't regularly check their email.

In circumstances where it is impracticable to notify individuals or groups affected, the Bill provides that an organisation will not be required to provide direct notice.

Instead it must publicise notification information on its website. But the

Bill does not stipulate what constitutes such circumstances or the extent of the "publicity" required.

This leaves open the possibility that breach notifications will be relegated to some deep, dark corner of the websites of less scrupulous organisations.

Who must act?

While the changes to the Privacy Act target businesses and government agencies, there are also some limitations concerning the groups to which the law applies.

Worryingly, the breach notification requirements only apply to those organisations covered by the original Privacy Act.

However, this means that state government organisations and local councils, and organisations with a turnover less than A$3 million a year do not need to comply with the legislation.

But the first two of these hold highly confidential data and are likely to be seen as easy targets by malicious hackers.

Foreign businesses serving Australian clients must comply with the law. But the Australian government lacks effective means to pursue breach information from multinational technology giants headquartered overseas if they are reluctant to comply. These is likely to be of concern if you use such services for email or data storage of personal information.

Law enforcement agencies that believe public knowledge of a breach might prejudice operations are also exempt. But a compromise of sensitive information held by such agencies can be more damaging than

information held by private organisations.

Data breach detection

By far the biggest problem with the new legislation is that it fails to recognise that breaches often go undetected for long periods of time. This offsets any benefit that might eventually be gained by reporting and notification.

The median number of days that attackers were present on a victim's network before being discovered dropped from 205 days in 2014 to 146 days in 2015, according to a report from US cybersecurity firm Mandiant.

This is certainly an improvement of the 416 days back in 2012, but is still of great concern.

Any damage that is going to be done is likely to occur within the first few days or months. Mandiant also reminds us that these are median figures and that some breaches still often go undetected for years.

Proactive action needed

What's needed is more proactive legislation, something between what is being implemented in Australia and that was recently implemented in China which has a set legal principles for protection of personal data.

So businesses offering products and services here could be required to obtain consent when collecting user information, and be subjected to continual security maintenance and mandated health checks at set intervals.

Those holding critical data could also be required to hold it within Australian territory and perhaps even at dedicated (highly protected) sites.

Moving beyond what China has done, it would also be wise to mandate network operators and major data holders to establish and maintain broader business continuity and cyber security incident response plans.

In the case of attacks leading to data breaches, they could then report to a governmental department that would non-selectively provide live website updates on recent incidents for public consumption.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: New law will force some (but not all) organisations to reveal data breaches (2017, March 10) retrieved 24 May 2024 from https://phys.org/news/2017-03-law-organisations-reveal-breaches.html