
# OUT OF THE SHADOWS:

## Data breach mandatory reporting and cyber insurance

A white paper by Ben Richardson,
Specialist Cyber Insurance Underwriter

QBE

## Introduction

On 13 February 2017 the *Privacy Amendment (Notifiable Data Breaches) Bill 2016* passed both Houses of Parliament. Once it is given royal assent it will amend the Privacy Act 1988 and impose mandatory reporting obligation on certain businesses for eligible data breaches.

The obligation to report data breaches has the potential to be costly for Australian businesses. This is because of the likely need for organisations, in the case of a breach, to undertake forensic investigations, establish contact centres, and notify affected customers. In addition to the upfront costs to the business, there's potential to suffer reputational damage and litigation if a business's response is handled poorly.

Now is the time for businesses to explore the capabilities of cyber insurance policies which offer indemnity for the mandatory notification provisions introduced with the passing of the new legislation. Defending against potential breaches will be a difficult task as a business will need to factor in both malicious and non-malicious threats from both an internal (employee error) and external (hackers) perspective. But to be considered for cover, cyber underwriters will continue to require strong evidence that businesses have internal risk management policies already in place.

## The legislation: at a glance

### Who does it apply to?

Businesses with an annual turnover of more than $3 million, health service providers, credit reporting bodies, credit providers and tax file number recipients.

### What constitutes an "eligible data breach"?

An unauthorised disclosure of, access to or loss of personal information which a reasonable person would believe would likely result in serious harm to the person whose information has been affected.

According to lawyers at Wotton and Kearney[1] the question of 'serious harm' will need to be considered in light of:

- The type of information which has been disclosed, accessed or lost as a result of the breach, as well as the sensitivity of the information.
- What security measures were in place to protect the data and the likelihood it could be breached (for example, was the data encrypted and how easily could someone decrypt it?).
- Who could get access to the data and what kind of harm could result (for example, identity theft, extortion, financial exposure).

The Bill outlines further factors that need to be considered and also notes that 'any other relevant matters' should also be considered. The list above is not exhaustive in determining what amounts to 'serious harm'.

### Investigations and notifications

Businesses must carry out a reasonable and expeditious assessment as to whether an 'eligible data breach' occurred and this must take place within 30 days after it first suspects such a breach.

### Who needs to be notified?

The Privacy Commissioner and individuals affected by the breach must be notified as soon as possible. If it's not practical to notify affected individuals directly, a notice can be published on the business's' website and other public forums, for example in a newspaper, on television or through digital media.

### What needs to be notified?

The notification should contain:

- Details of the business, the subject of the breach and any other organisations which may also have been affected by the breach.
- A description of the breach itself and the information affected by the breach.
- Recommendations about what steps affected individuals should take in response to the breach, for example, cancelling credit cards that may have been compromised.

### Do all breaches need to be notified?

Some circumstances won't require notification as it won't be considered an "eligible data breach". According to Wotton and Kearney, the circumstances depend on whether the affected business took remedial action to prevent the unauthorised disclosure, access or loss of information resulting in 'serious harm'; and if a reasonable person believes no such 'serious harm' would likely occur to the affected individuals.

### Are there penalties for noncompliance?

The Bill doesn't include civil penalties for noncompliance. However, according to Wotton and Kearney, breaches are subject to the existing powers of the Privacy Commissioner.

> **"Cyber underwriters** will continue to require strong evidence that businesses have internal risk management policies already in place."

[1] The advice in this section is based on analysis provided by Andrew Moore and Ahrani Ranjitkumar, of Wotton and Kearney. Wotton and Kearney provide legal advice to QBE customers about privacy and cyber breaches.



## What is cyber insurance?

Cyber insurance is relatively new in the Australian market, and provides indemnity for a range of first party exposures as well as coverage for third party claims arising out of cybercrime, network, and data security related events.

Cyber wordings include cover for forensic investigation costs, asset rectification costs, business interruption cover, public relations consultancy costs, and extortion costs, and also provide indemnity for the associated notification costs following a data breach. This class of insurance has been developed to complement and work alongside strong internal security capabilities to ensure businesses can continue to trade without being burdened by the immediate cost arising from any data breach or network security event.

Cyber insurance has been prevalent in the US market since the early 2000s, with the first mandatory breach legislation coming into effect in California in 2003. Even without official mandatory breach legislation, the Australian market was an early adopter of cyber insurance in some sectors, although general take-up to date has been moderate with a lot of businesses remaining hesitant to purchase a cyber policy. This legislative change brings us in line with the legislative environment in the US market, and we now expect this to lead to a maturing and growing Australian cyber insurance market.

The insurance implications of the Australian legislation will reach further than just standalone cyber insurance policies. This is because cyber exposure has the potential to overlap with other traditional lines of insurance, the most notable being directors and officers insurance. The Bill further cements data security exposure as a risk issue that all company boards must address. This means, certainly as far as larger ASX-listed companies go, if the data breach is serious enough to affect the share price or a specific class of individuals, for example, employees, then legal and regulatory action against directors and officers will move into scope. More than ever, company boards will need to ensure they are well across their business's security practices and encourage a strong security culture to avoid being placed in the firing line.

## Cyber underwriting and the risk analysis process

Increased claims costs associated with the notification provisions under the new legislation means underwriters will continue to place a greater focus on risk management and internal culture when they're reviewing risk.

A strong internal security culture can be the most effective defence against threats. But judging business culture on the basis of an insurance proposal form is notoriously difficult.

For this reason, underwriters will look favourably on certain business capabilities that indicate a strong security culture, including:

- Internal data handling and internet usage policies for all employees across the business. This will ensure data is managed in a safe and consistent manner while also preparing employees to identify and escalate potential incidents as soon as possible.
- Adequate prevention, detection, and response security capabilities to defend from external threats. Prevention measures will defend from known threats, while detection and response measures will ensure the business can quickly identify any newly found anomalies or threats and respond in a swift manner.
- Internal data breach incident response plans demonstrate the business has pre-planned its response to get ahead of the legal, reputational and financial repercussions.

SMEs of any size, including those not subject to the new legislation, hold a lot of exposure to data breach and cybercrime events, which can lead to business interruption, expensive forensic investigations, or third party liability claims. In today's connected age, an SME is also likely to have access to customers all over the globe and can still collect large volumes of customer data, which needs to be protected. This means underwriters will still expect strong risk management procedures to be in place for SMEs seeking cyber cover, regardless of whether they're subject to the new mandatory data breach reporting obligation.

**Ben Richardson is an underwriter with QBE Insurance Australia in the Professional and Financial Services Lines, specialising in cyber insurance.**

For more information about cyber insurance visit qbe.com.au/business/insurance-for-businesses/business/professional-liability