HERBERT SMITH FREEHILLS

DATA BREACH NOTIFICATION LAWS REINFORCE EMPHASIS ON CYBER SECURITY STRATEGIES

17 February 2017 | Australia
Legal Briefings – By **Merryn Quayle** and **William Hanna**

Companies across Australia must review their corporate governance and cyber security strategies to ensure they meet the increased regulatory burden following the introduction of a new mandatory data breach notification scheme.

On Monday the Australian Government passed amendments to the *Privacy Act 1988 (Cth)* to include mandatory notification of eligible data breaches to the Australian Information Commissioner and affected individuals.[1]

Now that transparency about cyber security breaches is a legal obligation for most large entities (the new law applies to private sector organisations with an annual turnover of more than $3 million and their related entities), it brings Australia into alignment with other countries which have had similar requirements for a number of years.

While many companies have been on the front foot in adopting comprehensive and transparent policies and procedures for cyber breaches, there were concerns under the previous voluntary notification system that data breaches were being underreported or notification delayed by some companies due to concerns that disclosure may adversely affect their reputation or create legal or commercial liabilities.[2]

Although voluntary notifications have increased in the past five years, the Office of the Information Commissioner predicts, based on comparisons with other jurisdictions, that notifications under a mandatory data breach notification scheme would nearly double to around 200.[3] In addition to the financial and reputational cost of a cyber breach, serious or repeated breaches of the reporting obligations will now also carry a potential civil penalty of up to $1.8 million.

IMPROVING CORPORATE GOVERNANCE

The additional compliance burden imposed by the new laws, on top of corporate disclosure requirements and director's duties that may already apply, is another step in the trend towards elevation of cyber security and data issues to the highest levels of corporate governance. Companies are increasingly aware of the risks posed by cyber and data security, including potential regulatory investigations, financial cost and reputational risk. Cyber issues are no longer viewed as a "tech" threat dealt with by IT teams or even an issue for senior management but as a risk management issue that affects the entire organisation and requires board oversight.[4]

Although directors understand the need to remain properly informed, wider research on the governance of cyber security suggests that, at present, many board executives have inadequate awareness of the full implications of digital threats to their organisations. One survey found that more than 90 per cent of corporate executives said they cannot read a cyber security report,[5] preventing them from asking the right questions and from being properly aware of the risks and implications of a breach. While each company's particular approach to cyber risk will differ depending on the industry and their risk tolerances, taking a proactive approach to improving cybersecurity governance can only assist with positioning companies and their boards to better address the risks and consequences of a cyber security breach.

BE PREPARED

In light of the new legislative changes, organisations will need to take the time to define what an 'eligible data breach' is in the context of their business and clearly designate who is responsible – both internally and externally – for managing and containing breaches and making the now mandatory notifications.

In addition to the usual network and IT security measures undertaken by many organisations to ensure protection against external and internal information breaches, organisations should ensure that they establish and maintain a comprehensive and up-to-date information risk management regime and incident response capability. This should include representatives from all relevant internal (and external) stakeholder groups, including a technical team to investigate any breach or suspected breach, HR and employee representatives, public relations and legal representatives, and the board.

Cyber security strategies and incident response plans should also be regularly reviewed and tested to ensure that they adequately address procurement and supply chain risk – including third-party service provider and information sharing arrangements. The Government has said that under the new regime, if more than one entity jointly holds the same personal records, an eligible (notifiable) data breach by one entity may also be a breach by the other.[6] This situation could foreseeably arise in cases involving corporate due diligence, outsourcing, joint ventures or share services arrangement and highlights the importance of taking the time to identify and manage these risk areas.

ENDNOTES

1. New mandatory Data Breach reporting law passed.
2. Australian Cyber Security Centre 2016 Threat Report, page 13 .
3. Privacy Amendment (Notifiable Data Breaches) Bill 2016, Explanatory Memorandum [69].
4. The Australian federal government's Cyber Security Strategy suggests "cyber security is a strategic issue for leaders – ministers, senior executives and boards – not just for IT and security staff." (Commonwealth of Australia (2016). Australia's Cyber Security Strategy, page 22). See here.
5. Tanium & NASDAQ (2016). Accountability Gap: Cybersecurity and Building a Culture of Responsibility.
6. Privacy Amendment (Notifiable Data Breaches) Bill 2016, Explanatory Memorandum [115].

LEGAL NOTICE