Article Information

Author: Tim Clark
Service: Corporate & Commercial

Data Breach Response Planning: Getting Down to Business

In the recent articles, Piper Alderman has discussed the needs for organisations to put in place suitable policies and plans in place to address information security risks.

In the recent articles, Piper Alderman has discussed the needs for organisations to put in place suitable policies and plans in place to address information security risks. The firm's recent article 'Count down to the introduction of the mandatory data breach notification obligations' provided an overview of the new mandatory data breach notification regime which comes into effect in February 2018. If you are unaware of the new data breach notification regime or whether it applies to your organisation, you should review that article.

In this article, ***Tim Clark, Partner****, and* ***Andrew Barling, Senior Associate****, outline some practical aspects for consideration by organisations to assist with data breach response planning under the new regime.*
Diary date reminder: Thursday, 22 February 2018

This is the date from which organisations falling under the *Privacy Act* 1988 (Cth) will have the obligation to notify individuals and the Commissioner of "eligible data breaches".

What's an eligible data breach?

This is more than just a legal definition. Each organisation needs to consider what this means and include a practical description in their data breach response plan so that staff know what to look out for, including where a data breach is only suspected but has not yet been confirmed. For example, the scope of the mandatory data breach notification is not limited to electronic records but also covers paper files, media and other tangible records.

New policy or update an existing one?

Organisations are likely to (or should) have existing IT, security and crisis management policies in place. Responding to an actual or suspected data breaches may involve consideration of issues that are already partially covered in such policies. Consider whether to create an entirely new policy or plan for data breach notifications or whether it would be more appropriate to amend an existing policy to include specific details around data breach notification.

Who's on the response team?

Organisations need to consider how they will resource and manage their response activities and who should drive each activity. For example, data breach notification plans should specify a clear escalation path for staff to enable rapid and effective escalation of any actual or suspected data breaches. The plan should detail how a response team is formed, who should be on that team and the roles and responsibilities of each team member.

Don't just 'have a policy'

As a general concept, having board-approved policies in place is a good, if not essential, practice for directors in discharging their directors' duties. But adopting a pro-forma policy may not be enough. Directors are expected to know their particular industry's typical risk management approaches and should be ensuring that they are incorporated into their organisation's risk systems. What is appropriate in one industry may not be appropriate in another.

One practical upshot of this when framing a data breach response plan is the need to consider whether other industry-specific regulators or stakeholders should or need to be notified (besides the Commissioner and affected individuals) in event of a data breach. By way of example:

- APRA-regulated institutions must notify Australian Prudential Regulation Authority of, amongst other things, major disruptions that have, or may have, a material impact on the institution's risk profile.
- Healthcare providers and operators have specific reporting obligations in relation to health information and health records under various State and Commonwealth legislation.
- Government departments and agencies may have specific statutory reporting obligations under governing statutes.

How will you approach notification where other parties are involved?

When complying with its notification obligations under the *Privacy Act* (Cth), an organisation has the option (under new section 26WK(4)) of naming other entities it has reasonable grounds to believe may also be involved in the data breach. Example scenarios discussed in the Commissioner's guidance include where the organisation outsources the handling of personal information, has a shared services arrangement with another entity or is involved in a joint venture.

The Commissioner's suggested online notification form includes an optional section to capture details of such entities. However, we suggest careful consideration should be given before deciding whether to provide such details. Issues that organisations will need to consider include whether the organisation's contracts with customers or suppliers prevents disclosure of such information as confidential or whether there is a contractually agreed process for dealing with such issues. In appropriate circumstances, we have drafted provisions in contracts providing for a framework to deal with data breach notifications.

Help – I can't find our response plan!

Finally, a data breach response plan will not be of use if it cannot be found and used in a timely manner. Issues to consider are whether relevant staff will actually be able to read the data breach response plan if IT systems are down. Whilst it is often advisable to have a single individual coordinating a data breach response, consideration should be given as to how others in the organisation may timely need to access the data breach response plan in that person's absence from the organisation.

Next steps

This article outlines a few practical points for organisations to consider in preparing a data breach response plan. If you would like assistance in preparing such a plan, Piper Alderman would be pleased to assist you and your organisation.