Submission to the Serious Data Breach Notification Consultation

(Consultation closes 4 March 2016 — please send electronic submissions to privacy.consultation@ag.gov.au)

Your details

Name/organisation *(if you are providing a submission on behalf of an organisation, please provide the name of a contact person)*	Protiviti Pty Ltd Ewen Ferguson (Managing Director)
Contact details *(one or all of the following: postal address, email address or phone number)*	[contact details redacted]

Publication of submissions

In meeting the Australian Government's commitment to enhancing the accessibility of published material, the Attorney-General's Department will only publish submissions to this website that have been submitted electronically.

Our preference is that submitters complete this template and send it to privacy.consultation@ag.gov.au.

However, if submitters choose to provide a separate document, the following formats are preferred:

- Microsoft Word
- Rich Text Format (RTF)
- txt format.

Please limit individual file size to less than 5MB. The department may create PDF documents from the above formats.

The department will still consider hardcopy submissions received by mail, but these submissions will not be published on the website.

Confidentiality

Submissions received may be made public on the Attorney-General's Department website unless otherwise specified. Submitters should indicate whether any part of the content should not be disclosed to the public. Where confidentiality is requested, submitters are encouraged to provide a public version that can be made available.

Would you prefer this submission to remain confidential? NO

Your submission

Introduction

Protiviti welcomes the opportunity to comment on the Federal Government's exposure draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015.

Protiviti is a global business consulting and internal audit firm composed of experts specialising in risk, advisory and transaction services. We operate from 70 locations in over 20 countries and our more than 4,000 professionals serve over 60 percent of FORTUNE 1000® and 35 percent of FORTUNE Global 500® companies. Through our work in advising our clients on critical business problems in information security, data management, risk and compliance, and internal audit (amongst other solution offerings), we have strong, pertinent expertise to comment on the implications of the Federal Government's proposed legislation to introduce a mandatory notification scheme for 'serious data breaches'.

Our views

Protiviti welcomes the intent of the proposed law. We support the draft Bill's approach of seeking to balance the interests of individuals whose personal information has been compromised in a serious data breach, with the need to keep the compliance burden in check for organisations subject to the new requirements.

We agree that the key benefit of the proposed mandatory notification scheme is that it will enable individuals to take steps to reduce the likelihood of identity theft or fraud when their personal data is compromised. At present, larger data breaches may attract publicity. However for the majority of breaches, the absence of a notification obligation means that affected individuals will remain unaware that their data is compromised and will be denied the opportunity to protect their interests. The Bill will reduce this problem provided organisations adequately understand the circumstances when a 'serious breach' has occurred and are able to activate their obligation to notify.

Incentivise data security

The draft Bill's Regulatory Impact Statement states that a further benefit of a mandatory notification scheme is that it is likely to promote compliance with privacy obligations. The Regulatory Impact Statement notes that the reputational damage that can follow a high-profile data breach, and the commercial consequences of such a breach, can provide powerful incentives for organisations to improve security.

On this point, we do not agree that the proposed legislation will result in widespread improvements to data security. Organisations that are planning to improve security will do so anyway, however those that have no intention to, are unlikely to change their security posture directly as a result of the new legislation.

Despite the increasing occurrence of cyber-attacks across all types of organisations and existing fines of up to $1.7 million for breaches of the Privacy Act 1988, in our experience, many entities still do not have adequate controls in place to prevent data breaches or to detect them when they have occurred.

In our view, the introduction of the proposed mandatory notification scheme will have little direct influence on the current state of corporate data security. Many companies will continue to improve information security

regardless, because they recognise ethical and moral obligations to their customers, or because of the reputational (rather than financial) impact of notification. The breach notification scheme may contribute as part of a business case for companies that are already planning to improve information security, however, the potential fine of up to $1.7 million is not enough of an incentive in its own right for medium or large companies to change immature practices.

We note that the cost to upgrade information security practices to the standard required to identify a breach, or reduce the likelihood of one occurring, would in fact, likely cost multiples of the penalty amount for medium/large companies. This predisposes companies to run the risk of incurring a data breach because the quantifiable penalties are relatively insignificant.

Accordingly, if one of the key objectives of the proposed data notification laws is to encourage entities to take greater preventative measures to secure personal data, the penalties for non-compliance, both under the existing Privacy Act and the proposed breach notification Bill, must be raised to a level that makes the cost of taking preventative action worthwhile. As noted above, many organisations will do the 'right thing' anyway in improving information security and for them a higher penalty would therefore be of limited concern.

Indicative benchmarks include the European Union's new General Data Protection Regulation which imposes a fine of up to 4 per cent of global annual turnover. Moreover, California law allows for civil action including class actions by parties affected by a data breach. These penalties represent stronger incentives for entities to take preventative action than those currently proposed by Australia's draft data notification Bill.

Recommendation 1: Increase the maximum penalty/fines under the draft Bill and current Privacy Act 1988 to a level that effectively encourages organisations to improve their data security, either in line with revenue or the scale of the breach. This recommendation is premised on the assertion that improving information security remains a desired outcome of the Bill.

Promote ease of compliance

We commend the draft Bill's emphasis on ensuring that the compliance obligations of organisations subject to the new notification laws are not unreasonably burdensome.

Nevertheless, in its current form, there are potential challenges in complying with the draft legislation. Unlike the European Union and United States regimes, where the notification triggers are more clearly defined, Australia's draft bill introduces more nebulous concepts that will require organisations to make more subjective judgement calls.

Ascertaining whether there are 'reasonable grounds' to believe a 'serious data breach' has occurred resulting in a 'real risk of serious harm' to affected individuals will be challenging in the absence of further guidance from the Privacy Commissioner about when these thresholds are met. After all, there is a wide spectrum of circumstances in which a data breach can occur, ranging from an employee losing a laptop containing a limited amount of non-financial personal information, to a large scale malicious theft of credit card details. There are a multitude of factors at play in any given case and it will not always be clear which are the most influential.

Furthermore, in many cases it may not be evident who was responsible for the breach, and how or for what purposes the data was compromised, making it difficult for companies to determine the severity and impact of the breach.

In any case where the facts are on the 'borderline' or where a case for non-disclosure is at least arguable, it is likely that organisations will opt against notification, to avoid the reputational impact of public scrutiny. We believe that a regime that encourages entities to 'err on the side of non-disclosure' does not adequately protect the interests of individuals affected by data breaches as potentially 'serious breaches' may go unreported.

This concern can be addressed in a number of ways.

Firstly, to assist organisations to accurately 'self-assess' their notification obligations, it is essential for the Commissioner to issue detailed criteria and case-study style guidance on how these concepts might operate in practice.

Secondly, there must be an avenue for entities to approach the Commissioner's office for prompt, in-confidence advice on whether their notification obligations apply in cases where the facts do not point to a clear outcome. This may be established as an administrative process by the Commissioner's Office or formally in legislation similar to the way federal tax legislation allows taxpayers to apply to the Australian Taxation Office for a binding 'private ruling' on how a tax law applies to their circumstances. In any event, the process must be an expedited one where the Commissioner commits to making a prompt determination, given that time is critical where data breaches are concerned and the consultative decision-making process should not unduly prejudice an individual's ability to take swift action where necessary, to protect their privacy.

Recommendation 2: Promote more accurate 'self-assessment' of notification obligations by requiring the Commissioner to issue detailed guidance

Recommendation 3: Establish an avenue for entities to approach the Commissioner for expedited advice on whether their notification obligations apply

Conclusion

The introduction of a mandatory data breach notification scheme in Australia is a welcome development given the rise in the frequency and severity of cyber-attacks and the unquestionable importance and value of information assets. The existence of such a scheme will bring Australia into line with other developed nations, notably, the United States, European Union, Canada and New Zealand.

The success of the proposed regime will be measured by its ability to:

- Ensure individuals are made aware of serious data breaches that affect them,
- Encourage organisations to take preventative measures to improve their data security and breach detection systems, and
- Simplify compliance by making it easy for organisations to understand and apply their notification obligations.

Our recommendations are intended to achieve these ends.

We thank you for the opportunity to provide our views and would be pleased to discuss these issues further.

- END –