www.pwc.com.au

PwC Submission

Serious Data Breach Notification Consultation

March 2016

pwc

Submission to the Serious Data Breach Notification Consultation

Your details

Name/organisation *(if you are providing a submission on behalf of an organisation, please provide the name of a contact person)*	**Business Name:** PricewaterhouseCoopers (PwC) **ABN:** 52 780 433 757 **Registered Office Address (for Company):** PricewaterhouseCoopers Darling Park Tower 2 201 Sussex Street Sydney NSW 2000 **Postal Address:** GPO Box 2650 Sydney NSW 1171
Contact details *(one or all of the following: postal address, email address or phone number)*	**Contact for inquiries:** Peter Malan, Partner **Phone no:** (03) 8603 0642 **Email:** peter.malan@au.pwc.com **Contact for inquiries:** Richard Bergman, Partner **Phone no:** (02) 8266 0053 **Email:** richard.bergman@au.pwc.com

Confidentiality

Would you prefer this submission to remain confidential? NO

Commercial and Administrative Law Branch
Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600

4 March 2016

Dear Sir/Madam,

PwC submission – Serious data breach notification consultation

PwC Australia ("PwC") welcomes the opportunity to provide comments on the *Mandatory Data Breach Notification Discussion Paper* and the exposure draft of the *Privacy Amendment (Notification of Serious Data Breach) Bill 2015* ("Proposed Bill"). This is an important Proposed Bill for the digital economy and the protection and security of Australian citizens' personal information.

PwC has significant experience helping the public and private sector prevent and respond to data breaches. Over the past five years, we have seen that the number of cyber security incidents have increased significantly.

Worldwide, PwC employs more than 3,000 cyber investigative, privacy, security and risk services professionals from a diverse range of backgrounds. Our team includes several individuals who have served in corporate roles such as the Chief Privacy Officer and Chief Information Security Officer across a variety of industries and organisations. PwC has a leading privacy and cyber security practice as recognised by organisations such as *IDC and Forrester*. We believe that our experience of working with a wide range of entities across different industries and geographies equips us with pragmatic insights on the potential impact of mandatory data breach notification in Australia and has informed our submission on the Proposed Bill.

Technology disruption continues at an unprecedented rate and is associated with the significant rise in privacy and security incidents. PwC supports the important role that mandatory breach notification plays in building and maintaining trust in the digital economy. This Proposed Bill will help align Australia with other jurisdictions leading in this area, such as European Union, some states in United States, and Canada. However, we also believe that there are areas that can be improved in the Proposed Bill to provide additional clarity and mitigate potential uncertainties if the Proposed Bill is enacted.

Our submission details several areas where we believe the Proposed Bill requires amendment or clarification to effectively meet its objectives. A summary of these areas has been provided below:

1 **The threshold of *'real risk of serious harm'*** – Entities will likely struggle to make an assessment of the seriousness of harm, given that individuals impacted by the breach may have varying tolerances for what is deemed harmful to them. We recommend that a 'reasonable person' test be introduced together with further guidance.

2 **Ought reasonably to be aware** – Based on PwC's experience working with entities of varying sizes and maturity, this is an area where entities may differ with the Office of the Australian Information Commissioner ("OAIC") on when the entity '*ought reasonably to be aware*'. We recommend that the OAIC issue additional guidance on this.

3 **As soon as practicable and the 30 days assessment period** – It is a balancing act between the practicality of the time required to investigate and confirm a potential breach and the Proposed Bill's objective to equip an individual with timely information to mitigate harm. We recommend that there is further clarification on the operation of paragraphs 26WC(1) and (2) of the Proposed Bill, together with the ability for entities to seek an extension to the 30 day timeframe in cases when their investigation is inconclusive within the 30 day period.

4 **Intelligible information** – Numerous forms of encryption and obfuscation techniques are available and provide vastly different levels of protection. We recommend further clarity be provided on encryption measures, taking into account how the data is compromised (i.e. lost vs. hacked) and the type of attacker (i.e. 'sophisticated' vs. ordinary person) that would attempt to compromise the data.

5 **Entities vs. contracted service provider responsibilities for notification** – The Proposed Bill applies to Australian Privacy Principle (APP) entities which '*hold*' personal information, however information may be both held and controlled by the outsourcing entity or processed and held by another entity. Clear definition on the entity responsible for notification should be provided.

PwC welcomes the opportunity to discuss our submission with you further.

Yours sincerely

Peter Malan
Partner

Richard Bergman
Partner

PwC submission

PwC supports the introduction of mandatory serious data breach notification in Australia.

Some of today's most significant business trends, including the explosion of 'big data', the digitisation of business processes and the 'Internet of Things' have expanded the importance of technology and data. Coupled with the sophistication of the dark web and the persistence of threat actor groups, Australian entities are facing more risk than ever before. With huge volumes of personal information about Australians now being collected by entities around the globe, there is increasing expectation around the protection and use of that information from consumers, including increased transparency when a breach of security of personal information occurs.

As part of our research we have leveraged our survey of more than 10,000 Chief Executive Officers, Chief Financial Officers, Chief Information Officers, Chief Information Security Officers, Vice Presidents and Directors of IT and security practices from more than 127 countries (*The Global State of Information Security® Survey)*. This survey highlighted that the number of detected information security incidents rose at a staggering 38% over the last 12 months.

There is growing concern among senior executives and boards within Australia regarding the potential damage to reputation, class action lawsuits and costly business interruption as the result of a serious cyber breach. Investing in better security and privacy incident management practices will assist entities to be better equipped to assess and respond to breaches in a more effective manner, mitigating the risk of reputational damage, financial harm and penalties, and serious harm on individuals. In an economy where trust is the new digital currency, entities have become increasingly aware of the need to build sustainable relationships with consumers through resilient and secure information management practices.

Based on PwC's breach response experience, we know that despite the best efforts of organisations and their partners, breaches do occur. We also know that when the breach is not public knowledge, the topic of notification has always been a difficult one. Organisations in the United States that have, in recent years, been the subject of data breaches have become the subject of international news (often after mandatory notification). Australian entities that would be subject to mandatory data breach notification requirements arising from the Proposed Bill are likely to fear the reputational damage that accompanies reporting a breach publicly.

However, in light of the current privacy and cyber security risk landscape and increasing consumer expectations, we believe the mandatory serious data breach notification requirement will support transparency between Australian entities and individuals. It will serve to encourage entities to take appropriate action to mitigate serious harm for affected individuals and adopt appropriate actions. The introduction of a mandatory reporting obligation will also place Australia in line with other jurisdictions seen as leading in the protection of privacy and data security, such as Canada, European Union, and certain states in the United States.

Although guidelines issued by OAIC currently encourage voluntary data breach notification, the mandatory nature of obligations in the Proposed Bill will serve as a timely reminder to Australian entities of their responsibility and accountability in managing the personal information they hold. It is likely to encourage more stringent adherence to *APP 11* on security of personal information and therefore better protection of individuals' personal information.

Although PwC supports the introduction of mandatory serious data breach notification in Australia, this submission details several areas where we believe the Proposed Bill requires amendment or clarification to effectively meet its objectives of providing greater certainty to consumers while providing entities with certainty on the implementation of the obligations. These areas are as follows:

1 **The threshold of '*real risk of serious harm*'**

2 **Ought reasonably to be aware**

3 **As soon as practicable and the 30 days assessment period**

4 **Intelligible information**

5 **Entities vs. contracted service provider responsibilities.**

Contents

1 The threshold of 'real risk of serious harm'

A threshold should be set to require notification of a serious data breach when the personal information specified in the regulation is subject to unauthorised access or disclosure. The exposure draft proposes that the threshold of the '*risk*' of '*harm*' to the individual(s) affected must be '*serious*' in order to require notification to affected individuals and the OAIC. Whilst the terms real '*risk*' and '*harm*' have been defined respectively in paragraphs 26WF and 26WG, the threshold of the '*seriousness*' of harm to determine notification has not been defined.

In our view, entities will struggle to make an assessment of '*seriousness*' given that individuals impacted by the breach may have varying tolerances for what is deemed harmful to them. Further, entities will struggle to determine when unauthorised access or disclosure of personal information may result in psychological, emotional, or reputational harm, for the individuals affected, as these categories of harm are more difficult to capture and measure.

What is seen as serious harm from one perspective may not be from another and the consequence of a data breach can often be unpredictable and speculative until actual harm occurs. Investigation of a reported breach will not lead to absolute certainty of all possible outcomes for the individuals impacted by the breach.

Some of the subjectivity could be removed or mitigated, for example, through introduction of a '*reasonable person*' test, or the introduction of objective criteria.

Recommendation

Further guidance should be provided in the Proposed Bill or explanatory memorandum to enable entities to implement a consistent and repeatable process for breach notification that enables them to determine whether the threshold of a '*real risk of serious harm*' has been met, and therefore whether mandatory reporting is required.

Despite indication that guidelines may be introduced to provide direction as to what would constitute '*serious harm*', in our view an additional paragraph should be included in the Proposed Bill to provide relevant matters to consider when determining what will constitute harm that is '*serious*', including specifically a '*reasonable person*' test. We note other jurisdictions provide either clear examples of what is considered as the '*risk of serious harm*' or quantitative/qualitative measures of unauthorised access or disclosure which trigger notification requirements.

2 Ought reasonably to be aware

According to the Proposed Bill, the notification obligation and response period is triggered when the entity '*is aware, or ought reasonably to be aware, that there are reasonable grounds to believe that there has been a serious data breach of the entity*'.

Based on PwC's experience working with entities of varying sizes, each entity's maturity in privacy and security incident management differs, and as such, their capability in detecting privacy or security incidents also differs. According to PwC's *Global State of Information Security Survey (GSISS)*[1], it takes an average of 243 days between an entity being hacked and it detecting the compromise. This equates to more than six months that an attacker can spend within a network, completely undetected or unrestricted.

As such, we identify this as an area where entities may differ with the OAIC on when the entity 'ought reasonably be aware' that there are reasonable grounds to believe that there has been a serious data breach. It would especially be a challenge for smaller entities - with less mature privacy management frameworks, less resources to manage privacy and security programs of work and less sophisticated tools and technology to detect a breach.

For example, if the entity experiences a customer complaint on social media or a specific alarm within an IT system, the implications of these singular events may not come within the consciousness of someone within the entity that those events have significance in relation to awareness of a serious data breach. It is not clear whether the OAIC would regard those events as being sufficient to form the view that the entity ought to have been reasonably aware that there were reasonable grounds to believe that there was a serious data breach.

Recommendation

In our view, additional guidance should be provided by the OAIC as to the circumstances they would consider an entity to ought reasonably to be aware there has been a breach. Case examples can be provided as additional notes under the clause, or included as an additional clause to the Proposed Bill. Failing the amendment, such circumstances should be at least outlined in guideline or information sheets by the OAIC.

1 The Global State of Information Security® Survey is a worldwide study by PwC, CIO, and CSO. Readers of CIO and CSO and clients of PwC from around the globe were invited via email to take the survey. The results discussed in this report are based on responses of more than 10,000 CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security practices from 127 countries. Thirty-seven percent (37%) of respondents are from North America, 30% from Europe, 16% from Asia Pacific, 14% from South America, and 3% from the Middle East and Africa. The margin of error is less than 1%.

3 'As soon as practicable' and 30 days timeline to assess breach

The notification timelines in international breach notification regulations vary significantly. Some jurisdictions prescribe notification to be made as soon as reasonably possible (without providing a specified date), while other jurisdictions prescribe a specific period. For example in the United States, the requirement to notify ranges from no later than 30 days to as soon as reasonably possible, while in the proposed European Union General Data Protection Regulation ("*EU GDPR*") the requirement to notify is 72 hours from identification of a breach.

Paragraphs 26WC(1) and (2) of the exposure draft of the Proposed Bill appear to provide leeway for entities to utilise a 30-day window prior to notifying affected individuals and the OAIC.

We often find that where a data breach is suspected by a larger entity the investigation may take longer to complete. In the event that it is a complex breach, and as a result the investigations may go well beyond the 30 day threshold currently set out in the Proposed Bill.

As was the case with some high profile credit card security breaches in the US, there may be a need to modify and re-report the details of a breach multiple times once additional information is obtained throughout the investigation.

One of the main objectives of the Proposed Bill, which is to equip affected individuals with the power to mitigate harm caused to them, needs to be balanced with an entity's ability to quickly investigate and assess a breach.

Recommendation

Clarification should be provided that paragraphs 26WC(1) and (2) of the Proposed Bill provides a 30 day timeframe only for entities which are unsure of a confirmed breach, and therefore require additional time to investigate and assess the incident. In other circumstances, the entity should report as soon as they confirm the breach within the 30 day timeframe.

Additionally, we recommend that entities should be able to apply to the OAIC for an extension to the 30 day timeframe in circumstances where the investigation of the breach is inconclusive. For example, an entity may not have been able to determine the cohort of individuals to whom the breach relates and needs extra time to do so. Without such an extension, notification at 30 days would be non-specific to affected individuals and would need to apply to a larger, potentially unaffected set of individuals. The OAIC would be required to assess the implications of the extension against the potential risk to individuals and their ability to mitigate harm in the intervening period.

4 Intelligible information

Sections 26WB(3) (c) and (d) requires entities, as part of determining if there is a *'real risk of serious harm'*, to *'have regards to... whether the information is in a form that is intelligible to an ordinary person'* and *'if the information is not in a form that is intelligible to an ordinary person – The likelihood that the information could be converted into such a form'*.

The consultation draft of the Explanatory Memorandum to the Proposed Bill at paragraph 45 states *'if the encryption method used could be circumvented – Which could occur if the encryption algorithm is out of date or otherwise not fit for purpose and* ***could be broken by a sophisticated attacker****, or if the decryption key was also accessed or disclosed in the data breach – The risk could exist that the information could be converted into a form intelligible to an ordinary person. Even where none of these concerns apply in relation to encrypted information, the entity may need to consider the likelihood of the encryption algorithm* ***being broken in the long-term****'*.

This reference in the draft Explanatory Memorandum, if used as a means to assist interpretation of sections 26WB(3) (c), would mean almost all breaches would require notification given entities suffering the breach may not have knowledge of who gained access to the data and/or the likelihood that data could be made intelligible would be reasonably high, particularly where a *'sophisticated attacker'* is concerned. We believe that the terms above in bold are problematic and do not assist an entity in practically assessing the real risk of serious harm.

These references also make consideration of the loss of encrypted information difficult. Numerous forms of encryption techniques are available that provide vastly different levels of protection. In some cases, encrypted information may be easily decrypted whereas other forms may take years to decrypt, though no practical encryption scheme can resist all possible attacks. If the encryption/decryption key can be obtained, then the strength of the encryption is irrelevant. Weak implementations of strong encryption methods can lead to the encryption being vulnerable to simple attacks.

The EU GPDR provides an exemption to entities from notifying individuals if it *'has implemented appropriate technological and organisational protection measures and those measures were applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption*'. This allows for entities to make a more practical assessment of whether a *'real risk of serious harm'* has been realised though it does not differentiate between information protected by *'cryptographically strong'* or *'cryptographically weak'* encryption algorithms.

Recommendation

Further clarification on clauses 26WB(3) (c) – (d) would be welcomed, specifically regarding the likelihood that information could be converted into a form that is intelligible to an ordinary person, including encryption and other technological protection measures. Particularly, we encourage further guidance to be provided that will address certain encryption mechanisms, taking into account how the data is compromised (i.e. lost vs. hacked) and the type of attacker (i.e. 'sophisticated' vs. ordinary person) that would attempt to compromise the data.

5 Responsibility for notification – Entities vs. contracted service providers

A common challenge we see facing our clients is how to determine accountability and responsibility for maintaining the security and privacy of personal information in an entity (the first entity) which engages external contracted service providers ("CSPs") to operate IT systems that process or store this information on behalf of the entity.

It is generally accepted that, having established the initial relationship with the consumer, the first entity has ultimate ownership and thus accountability for maintaining the security and privacy of the data entrusted to them by the consumer. However, as that data is often processed and stored in IT systems maintained by a CSP, the responsibility for implementing and operating adequate controls to protect that data is often the responsibility of the CSP. In this scenario, the first entity is expected to put measures in place to ensure that the CSP has effectively designed and is operating adequate controls.

The exposure draft of the Proposed Bill applies to APP entities which '*hold*' personal information and are required to comply with APP 11.1 relating to the protection of that personal information from '*misuse, interference and loss, and from unauthorised access, modification or disclosure.*' Based on the current wording in the exposure draft, a reasonable person might determine that a CSP which 'holds' personal information in systems operated and maintained on behalf of an entity would be expected to notify the OAIC of a serious breach.

Recommendation

We recommend that the Proposed Bill be amended to clarify who is responsible for reporting a serious data breach in the event that the information was '*held*' by a CSP. Our recommendation is that the CSP should inform the first entity of a potential breach, and that the first entity should be both responsible and accountable for notification once an investigation (by the CSP, the first entity or both) determines that a serious breach has in fact occurred. This approach is consistent with the incoming EU GDPR where the '*data processor*' (the CSP) is obliged to notify the '*data controller*' (the first entity), who is then obliged to notify the regulatory body.

6 Conclusion

In conclusion, we support the introduction of mandatory data breach notification. This submission details several areas where we believe the Proposed Bill requires amendment or clarification to effectively meet its objectives of providing greater certainty to consumers, while providing entities with certainty on the implementation of the obligations. These areas are as follows:

1 **The threshold of '*real risk of serious harm*'**

2 **Ought reasonably to be aware**

3 **As soon as practicable and the 30 days assessment period**

4 **Intelligible information**

5 **Entities vs. contracted service provider responsibilities.**

Our practitioners are available for further discussions or consultations in relation to the submission, and we welcome further opportunities to have ongoing conversations about legislation and issues impacting privacy and security in Australia.

www.pwc.com.au

At PwC Australia our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.au