Guidance Material: Serious Data Breach Notification

AIIA response

July 2017

Ground Suite B
7-11 Barry Drive
Turner ACT 2612

GPO Box 573
Canberra ACT 2601

T 61 2 6281 9400
E info@aiia.com.au
W www.aiia.comau

About AIIA

The Australian Information Industry Association (AIIA) is Australia's peak representative body and advocacy group for those in the digital ecosystem. We are a not-for-profit organisation to benefit members.

Since 1978 the AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment and to contribute to Australia's economic prosperity.

We represent organisations nationally, including global brands and a large number of ICT SMEs.

Comments

AIIA appreciates the opportunity to comment on this important issue. We support in principal, a mandatory serious data breach notification scheme.

Practically we agree that such a scheme:

- might help incentivise better data security measures
- might help prioritise and reduce the number of personal information collected and
- overall will better ensure greater reporting and consistency than the other options presented in the RIS

In our previous feedback to government AIIA raised a number of concerns and clarifications along with a list of recommendations.

This paper reflects on that feedback and assesses whether the updated guidance material of June 2017 adequately addresses the issues raised.

Issues raised relevant to the guidance material were:

- The definition of real risk of serious harm is unclear
- Notification should only be triggered where there is real risk of serious harm
- Third party responsibility is unclear – data processors vs. data controllers
- Current drafting of 'as soon as practicable' is overly strict
- Public interest exemptions are ambiguous and generally hard to establish

This paper also reemphases outstanding issues yet to be addressed:

- State & Territory Governments should be held to the same obligations – whether under this scheme or a separate arrangement
- Data collected should be published

The definition of real risk of serious harm is unclear

AIIA recommended:
• That any guidance material; be jointly developed and endorsed by industry; be clear and specific; and include weightings • Government clarify the intended scope of serious harm

The updated guidelines go some way to addressing this issue. However some concerns remain.

Under the heading 'Is Serious Harm Likely' the draft states that the "chance that an individual will experience serious harm increases as the number of people whose personal information was part of the data breach increases. It may therefore be prudent for an entity to assume that a data breach that involves the loss of personal information of a very large number of individuals is likely to result in serious harm to at least one of those individuals unless the context or circumstances would support this not being the case."

This assumption is highly questionable if measures such as commercially reasonable encryption, were used to protect the data set. Without being prescriptive, the OAIC should recognize that certain compensating security controls can reduce the risk of harm.

Under the heading "The Type of Personal Information Involved in the Data Breach," the OAIC lists as an example of the kinds of information that may increase the risk of serious harm if there is a data breach, "a combination of personal information (rather than a single piece of personal information)."

AIIA considers this to be inaccurate, as the risk is dependent on the nature of the data elements involved, not the mere fact that there are multiple data elements that are personal information present. For instance, if the breach involves name and gender, the risk of serious harm does not increase significantly in comparison to if only name or gender alone were to be impacted.

Under the heading "What is a 'Data Breach" it reads like the OAIC attempts to define "unauthorized disclosure" – which is not defined in the Privacy Act – as "when an entity makes personal information accessible or visible to others outside the entity, and releases that information from its effective control in a way that is not permitted by the Privacy Act."

When data is merely accessible – but not in fact accessed – there is no harm to data subjects (at least, insufficient harm as to constitute a data breach). The key distinguishing factor should be whether the entity has any way of determining if the data was, in fact, accessed. "Unauthorized disclosure" should be likened to publication, where the personal data is essentially published (e.g., sent to an entire mailing list comprised by a large number of recipients) and there is no way to know whether or not it was accessed. If the entity is able to determine, or reasonably believes, that the data in question was accessed, it would fall under "unauthorized access." If there is no way to know, it may be "unauthorized disclosure."

AIIA notes the guidance material does clarify that that the scope of serious harm also extends beyond material harm to include physical, psychological, emotional, economic and financial harm, as well as harm to reputation. While AIIA supports the broaden scope of harm, it's important that the test is not too remote that it ultimately lowers the threshold of when notification is triggered. This is significant given a key stated benefit of the Bill is its high notification threshold compared to similar international schemes and therefore is less of a regulatory burden. The guidance material should note this tension as part of the considerations.

Notification should only be triggered where there is real risk of serious harm

AIIA recommended:
• Delete sections 26WB(2)(a)(ii) and 26WB(2)(c) so that it is clear that notification is only triggered where there is a real risk of serious harm • Consider alternatives such as a self maintained 'Breach Register' and ability for the Commissioner to randomly audit such registers • Clarify that loss of unauthorised access to encrypted information is not subject to notification even if it contains personal information.

It's good to see that the guidance material clarifies that adequately encrypted, anonymised, or otherwise not easily accessible information is a consideration for when notification is required.

However under the heading "Examples of Data Breaches," Example 3, "Data Breach Experienced By Overseas Contractor Leading To Phishing," reads like a breach would be notifiable if a list of individuals containing name, email address, gender, and suburb were to be obtained by bad actors. The implication, is that the incident would be notifiable primarily because the entity learned that some of the data subjects were being phished.

AIIA recommend that OAIC make clear that this incident is only notifiable because of this specific knowledge, and that without this knowledge the incident would not rise to the level of a notifiable data breach.

Third party responsibility is unclear – data processors vs. data controllers

AIIA recommended:
• AIIA supports the EU approach which provides that the data processor is obliged to notify the data controller and the data controller obliged to notify the regulatory body.

It's good to see there is clarification on this point under 'data breaches involving more than one organisation.'

Current drafting of 'as soon as practicable' is overly strict

AIIA recommended:
• Expressly including that 'soon as soon as practicable' (under section 26WC(2)) includes a reasonable time to stop or contain the breach • Consideration should be given to the time required for data processors to notify principals and the principals to then notify the relevant individuals (this is addressed above).

Under 'Notifying individuals about an eligible data breach' the guidance states that "the Commissioner generally expects entities to expeditiously notify individuals at risk of serious harm about an eligible data breach unless cost, time, and effort are excessively prohibitive in all the circumstances."

This standard would alter the explicit language of the statute, which requires entities to notify the Commissioner and individuals "as soon as practicable." AIIA is opposed to any attempts to accelerate any such obligation to provide notice to individuals, as it is vital to confirm facts before rushing to provide notice. Not to mention the clear public benefits of entities taking reasonable time to stop or contain the breach.

Another issue relating to notification is the draft Australian Information Commissioner's role in the NDB scheme.

Under Section 26WK of the Privacy Amendment, the required contents of the notification to the OAIC and at-risk individuals are:

1. the identity and contact details of the notifying entity;
2. a description of the data breach;
3. a description of the personal information involved; and
4. recommendations to individuals about the steps that they should take to minimise the impact of the breach.

However, in the guidelines under the heading "**Receiving Notifications of Data Breaches" > "Responding to Notification**s,'" the OAIC states that the Commissioner's criteria for whether to "make inquiries or offer advice and guidance in response to notifications" include "the numbers of individuals potentially at risk of serious harm, and the extent to which the notification statement and any additional supporting information provided demonstrate that:

- the data breach has been contained or is in the process of being contained where feasible;
- the notifying entity has taken, or is taking, reasonable steps to mitigate the impact of the breach on the individuals at risk of serious harm; and
- the entity has taken, or is taking, reasonable steps to minimise the likelihood of a similar breach occurring again.

None of these criteria, are required to be reported to the OAIC by the Privacy Amendment. Although the guidance states that entities "may also provide additional supporting information to the Commissioner to explain the circumstances of the data breach and the entity's response in further detail," the OAIC makes clear that this is "not required by the Privacy Act." Effectively, any entity that does not provide this information, however, will be highly likely to receive further inquiries from the OAIC requesting this information. While it is not unreasonable for the OAIC to consider these criteria, it should be made clear that providing such information is not compulsory.

Public interest exemptions are ambiguous and generally hard to establish

AIIA recommended:
• Adopt the EU exemption (under 26WC(6) to 26WC(14)) so that an entity should not be required to issue a data breach notice in circumstances where an enforcement body advises the entity that such notice would prejudice ongoing investigations or enforcement activities.

It is disappointing that the guidance material does not address exemptions at this point.

While the rationale for a public interest exemption is clear and we want to avoid situations where the exemption becomes the rule, industry requires a certain level of reasonable exemptions to the scheme.

For example, following a serious data breach, the affected entity may need to cooperate with law enforcement investigations relating to the breach. In addition to the exceptions set out in section 26WC(6) to 26WC(14), some industry groups propose that an entity should not be required to issue a data breach notice in circumstances where an enforcement body advises the entity that such notice would prejudice ongoing investigations or enforcement activities.

AIIA supports this amendment.

AIIA recommends that entities should not be put in the position where they must either breach their obligations under the Scheme or refuse to comply with a direction from a law enforcement agency.

Under the current Bill, enforcement bodies are exempt from notifying affected individuals where the enforcement body reasonably believes that it would be likely to prejudice its enforcement activities (section 26WC(5)). To the extent an enforcement body directs an entity to take certain steps that entity should be entitled to at least the same exemption.

Other issues

State & Territory Governments should be held to the same obligations – whether under this scheme or a separate arrangement

A key success factor of the scheme is a consistent and national reporting framework. Currently state and territory governments hold significant amounts of sensitive information but are subject to different reporting requirements – if any - under various state based legislation.

AIIA recommends consistency and harmonisation with state and territory governments be a key focus for next steps.

Data collected should be published

An early driver for introducing data breach reporting is to improve cyber security by sharing information when a breach occurs. This keeps the business community on the lookout for attacks with the added advantage of sharing lessons learnt to reduce likelihood of it occurring again.

These drivers are still applicable. Without information sharing its arguable that the benefits of the scheme is largely reduced.

AIIA recommends that all data from this scheme should be made available annually, anonymous and in a user friendly format.