Serious Data Breach Notification

AIIA response

March 2016

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

However we have a number of concerns and clarifications with the proposed scheme which we outline below and provide a summary of recommendations at the end.

The RIS and discussion paper do not fully explore the alternatives

If the overall aim is to protect consumer information and empower consumers to take action when a breach occurs, there are a number of ways to achieve this short of a mandatory reporting scheme. The current options in the RIS go from do nothing, a mandatory scheme or industry codes as a middle ground.

AIIA considers that the options presented are narrow and other middle ground alternatives could have been explored. For example, one option might be random audits and naming and shaming. While AIIA is NOT proposing that we support these alternatives, we nonetheless consider it vital that analysis of these alternatives are done - in terms of their cost and effectiveness. This lack of information means industry cannot provide a fully informed view.

The definition of real risk of serious harm is unclear

Currently 'real risk of serious harm' is not defined in the Bill. Instead the draft Bill identifies several relevant matters that entities could take into account. The Bill also provides that entities could take into account any other matters that are relevant in the circumstances. Finally, it is expected that the Commissioner would issue guidance material.

AIIA considers the current approach is very broad and risks confusion, added complexity, delays and ultimately non-compliance. The Commissioner's latest guideline[1] contains a raft of suggestions and considerations without weightings to indicate which are critical. If all are critical, the material doesn't adequately indicate timing priorities.

AIIA recommends that any guidance material; be jointly developed and endorsed by industry; be clear and specific; and include weightings.

[1] Data breach notification — A guide to handling personal information security breaches, 2014, available at: https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches#step-2-evaluate-the-risks-associated-with-the-breach

AIIA members advise that a good example of guidance material for breach notification is ASIC's Regulatory Guide 78, Breach reporting by AFS licensees.

Having said that, on balance, AIIA agrees that a definition in the Bill is not the optimal approach. Rather clear guidance is required. A definition would necessarily restrict the scheme to the current settings. Whereas legislation that is flexible and adaptable to changing circumstances is much more suitable to regulating cyber security – an area of technology that by nature is constantly evolving.

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.

AIIA recommends that Government clarify the intended scope of serious harm.

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

Currently, the Bill provides that a serious data breach occurs even where there is no real risk of serious harm (sections 26WB(2)(a)(ii) and 26WB(2)(c)).

By requiring notification without this trigger, the scheme risks 'notification fatigue', where individuals are notified of data breaches when no serious harm is likely to occur, and they are unduly inconvenienced or fail to take appropriate action in response to those notifications.

Presumably the purpose of these provisions is to allow the Attorney-General to prescribe some categories of personal information as so sensitive that any breach should be notified. While there are merits to this approach, this is outweighed by the real risk of over complicating the scheme given the already complex test of 'real risk of serious harm' – which is undefined and self assessed. Moreover, this is not a feature of most notification laws in other jurisdictions.

An alternative might be a requirement for an entity to maintain a 'Breach Register' that would record the entities' 'justification' on whether the Commissioner is notified along with the ability for the Commissioner to audit the 'Breach Register'. This change would reduce the administrative burden on entities, reduce the prospect of notification fatigue and align with the intent of the Bill to ensure only serious data breach that poses a real risk of serious harm are reported.

AIIA supports the approach adopted by the EU in its ePrivacy Directive for electronic communications services.[2] Under that system, it expressly excludes from the notice obligation data that has been rendered unusable, unreadable or indecipherable through practices or methods, such as encryption, redaction, access controls or other such practices or methods, which are widely accepted as effective industry practice or industry standard. Currently it is unclear whether this exclusion also exists in the Bill.

A high level explanation of the EU scheme is provided at **Annexure A**.

AIIA recommends:

- **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**

[2] The ePrivacy Directive for electronic communications services has recently been extended to all businesses and organisations under the General Data Protection Regulation. For more information see: http://ec.europa.eu/justice/data-protection/reform/index_en.htm

- **Clarification that loss of unauthorised access to encrypted information is not subject to notification even if it contains personal information.**

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

Unlike other jurisdictions, the Australian legislation does not distinguish between data processors and data controllers i.e. the principal and a third party contractor. Proposed section 26WC(1) requires the entity to which the serious data breach has occurred to issue the notices.

However, AIIA notes that in practice personal information is commonly held by third party contractors. For example, with the increasing growth of cloud services, in many cases the entity that is holding or processing the information is a contractor of the principal entity that collected the personal information in the first instance and it is the principal entity that has the relationship with the individual.

As the bill currently stands, what this means in practice, is individuals could be notified of the one breach by multiple entities or be notified by an entity they didn't know held their personal information.

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 and the impacted individual.

This is consistent with the spirit of timely notification under the scheme, as a contractor likely does not have a normal mode of communication with the individual data subjects, where the principal likely does. This also simplifies the scheme for the individual as they'd be notified by a single entity with whom they have a relationship.

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

The Bill provides that 'as soon as practicable' (section 26WC(2)) includes the time taken by the entity to carry out a reasonable assessment of whether a serious data breach has occurred (provided that the assessment is performed within a certain amount of time).

However, there are other activities that should also be given similar allowance in determining what is 'as soon as practicable'. For example, in the event of a serious data breach, it's arguable that an equally important priority is to stop or contain the breach. If containing the breach is left until after a notification is issued, the risk of harm arising from the breach increases.

To be clear, this is not to say that braches can always be contained in a timely manner – this will depend on the nature and scope of the threat. For example a virus that is new will take longer to contain than a commonly existing one. As such 'as soon as practicable' should take into account the reasonable time required to contain the breach. **AIIA recommends that this activity be expressly included in the Bill.**

This is consistent with the EU scheme which provides that communication to the individual is not required if (among other things) the entity has taken subsequent measures which ensure that the high risk for the rights and freedoms of data subjects is no longer likely to materialise.

Also consistent with the above issue that 'third party responsibility is unclear' **AIIA recommends that consideration should be given to the time required for data processors to notify principals and the principals to then notify the relevant individuals.**

Public interest exemptions are ambiguous and generally hard to establish

While the rationale for this is clear and we want to avoid situations where the exception 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.

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.

Summary of Recommendations

AIIA recommends:

The definition of real risk of serious harm is unclear:

1. That any guidance material; be jointly developed and endorsed by industry; be clear and specific; and include weightings
2. Government clarify the intended scope of serious harm.

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

3. 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
4. Consider alternatives such as a self maintained 'Breach Register' and ability for the Commissioner to randomly audit such registers
5. Clarify that loss of unauthorised access to encrypted information is not subject to notification even if it contains personal information.

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

6. 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.

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

7. Expressly including that 'soon as soon as practicable' (under section 26WC(2)) includes a reasonable time to stop or contain the breach
8. Consideration should be given to the time required for data processors to notify principals and the principals to then notify the relevant individuals.

Public interest exemptions are ambiguous and generally hard to establish:

9. 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.

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

10. Consistency and harmonisation with state and territory governments be a key focus for next steps.

Data collected should be published:

11. All data from this scheme should be made available annually, anonymous and in a user friendly format.

Annexure A: Data Breach Notification under EU

In the EU, both the ePrivacy Directive and the General Data Protection Regulation introduce a 2 step approach for breach notification:

A. Under these regimes, the controller should without undue delay (after having become aware of the breach and, where feasible, not later than 72 hours after having become aware of it), notify the personal data breach to the competent supervisory authority, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals.

B. The individuals are solely notified if the personal data breach is likely to result in a high risk for the rights and freedoms of individuals, in order to allow them to take the necessary precautions. The communication to the data subject is not be required if:

   I. the controller has implemented appropriate technical and organisational protection measures, and that 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; or

   II. the controller has taken subsequent measures which ensure that the high risk for the rights and freedoms of data subjects is no longer likely to materialise; or

   III. it would involve disproportionate effort. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

C. EU law also provides that the breach notification regime must take into account the legitimate interests of law enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.