Mandatory Data Breach Notification Submission

AISA’s Response to the Commonwealth of Australia Attorney General’s

Data Breach Notification Discussion Paper
Executive Summary

As Australia’s leading organization of information security professionals, the Australian Information Security Association (AISA) is pleased to provide this submission in response to the Commonwealth of Australia Attorney-General’s Department Discussion Paper Mandatory Data Breach Notification (December 2015) seeking comment on the draft bill, Privacy Amendment (Notification of Serious Data Breaches) Bill 2105.

1.1. Summary of recommendations and findings

In summary, AISA submits as follows:

- Over 70% of members support the introduction of a mandatory data breach notification law on the basis that it will result in improved network and data security. However, members have indicated some concern as to their ability to apply the legislation as drafted in practice, which is discussed further below.

- Although AISA regards the introduction of a mandatory data breach notification law as a good ‘first step’, AISA recommends that consideration be given to further regulatory measures to encourage improved practices in relation to network and data security.

- AISA supports the annual publication by the Privacy Commissioner of details of cases where notifications have been issued to affected persons, suitably anonymised where relevant. This information will be invaluable in creating a better understanding of the Australian data breach landscape.

- AISA members have concerns regarding the proposed notification threshold and their ability to apply it. AISA recommends that the operation of the legislation be reviewed after 24 months to assess how effectively it is operating, on the basis of the proposed notification level.

- AISA recommends that some clarification be provided in regard to some of the terms used in the bill:

---

1 Discussion paper – Mandatory data breach notification [DOCX 318KB]
2 Exposure draft – Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 [DOCX 105KB]
• ‘Real risk’: AISA recommends clarifying the test of "real risk." A term such as 'possible' may provide more clarity than ‘not remote.’;

• ‘Harm’: AISA recommends that the emotional and psychological harm be defined by reference to an objective standard.

• AISA recommends that the Privacy Commissioner establish an expert advisory panel representing relevant stakeholders, including the information security community, to work with the Commissioner on identifying areas for clarification and developing relevant guidance and clarification. Such a panel would support the type of engagement between the regulator and the regulated community which is essential for the effective operation of a principle-based regulatory system, such as the Privacy Act 1988 (Cth).

• AISA recommends that the sunrise period for mandatory data breach notification to apply to information held by overseas recipients, not covered themselves by any data breach notification obligation, be increased to 3 years so that organisations have time to review and renegotiate the contractual arrangements necessary to ensure that they will have the information and investigatory powers necessary to ensure compliance.

• AISA recommends that a mechanism for identification of an appropriate reporting entity be included in the legislation.

• Members are divided on whether there should be a specific exemption for a data breach affecting encrypted information. AISA recommends that issues such as encryption be covered by additional guidance, developed in consultation with an expert advisory panel.

• The 30-day period provided for determining whether or not a serious data breach has occurred is regarded by most as a sufficient time period.

AISA thanks you for the opportunity to make this submission. We would be happy to engage in further discussion of any of the matters raised in this document.
1.2. Contacts Details

<table>
<thead>
<tr>
<th>Name/organisation</th>
<th>Australian Information Security Association (AISA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact details</td>
<td>Contact Person's Name: Arno Brok (CEO))</td>
</tr>
<tr>
<td></td>
<td>Contact Person's Mobile: [omitted]</td>
</tr>
<tr>
<td></td>
<td>Contact Person's Email: [omitted]</td>
</tr>
</tbody>
</table>
2. Introduction and Background

2.1. The Australian Information Security Association

The Australian Information Security Association (AISA) is a not-for-profit and charitable organisation formed to advance the cyber-security and safety of all sectors of Australian life; public, corporate, and government.

AISA’s vision is a world where all people, businesses and governments are educated about the risks and dangers of cyber-attack and data theft, and to enable them to take all reasonable precautions to protect themselves against it.

AISA is focused on individual professional membership with a current membership of around 3,000 security specialists. AISA aims to foster and promote the development of information security professionals and the security of the ICT industry.

Our broad membership base consists of information security professionals from all industries including education, finance, government, healthcare, manufacturing, mining, oil and gas, transportation, and utilities. Our members range from company directors and managers, lawyers, risk professionals, architects, highly skilled technical security specialists, professors and researchers.

2.2. Background to Data Breach Notification Submissions

As part of the AISA preparations for our response to the Government’s Cyber White Paper discussion paper in 2011, AISA surveyed its members on a number of information security related issues, including whether they supported the introduction of mandatory data breach notification in Australia. Based on the results of that survey, AISA submitted that:

- Data breach notification regulations should be introduced incorporating the lessons learned from the USA and EU experiences; and
- Any data breach notification scheme should be part of a broader and “more responsive” regulatory approach supporting information security.

Following the release of the Data Breach Notification Discussion Paper in October 2012, AISA again surveyed its members asking them to respond to the questions raised for consideration in that Discussion Paper. This included asking members to answer “yes”
or “no” to whether a mandatory data breach law should be introduced. Over 81% of members supported the introduction of a legal requirement for data breach notification. In the view of AISA members supporting the legislation, the main reason for introducing a data breach notification law is to act as an incentive for the organisations covered by the *Privacy Act* to improve data security practices.


In preparation for the submission of this document, AISA again surveyed its members, following a networked information session on the proposed legislation that included members from branches all around Australia. The questions posed to members in the February 2016 survey are included in Appendix A. Responses from 138 members were received. **Details of the actual member responses to these questions can be provided on a confidential basis on request.**

The results from the February 2016 survey were reviewed and findings and recommendations based on those results have been included in this submission.

AISA is proud to provide this further submission in response to the updated bill in February 2016, which incorporates the results of all surveys conducted previously and other consultations with members.
3. Findings and Recommendations

In this section, we outline the main findings based on the results of the member survey conducted in February 2016 and other consultations with members, together with previous survey findings and submissions made in regard to the introduction of a data breach notification law in Australia. Using all of this material, we also make submissions and recommendations in response to the draft legislation.

The findings, submissions and recommendations included in this document cover the following issues:

- Support for the introduction of the legislation;
- The notification threshold;
- Clarification of important terms including 'harm' and 'real risk';
- The treatment of mitigating factors, such as encryption; and
- The obligation to notify.

3.1. Support for introduction of the legislation

Members were asked two questions relevant to the general introduction of the proposed legislation:

- Would the legislation make their jobs easier or more difficult?\(^3\)
- Do you think a mandatory data breach notification law will result in improved network and data security?\(^4\)

While close to 40% of respondents believed their jobs would be made more difficult, 46% believed their job would be the same or made easier, with the balancing not able to say. This is perhaps consistent with the responses to the second question. A very strong majority of respondents, close to 72%, believed that the proposed mandatory data breach notification law will result in improved network and data security. These findings

\(^3\) 2016 Survey, Question 16.
\(^4\) 2016 Survey, Question 15.
are also consistent with findings in previous surveys to the effect that a majority of AISA members strongly support the introduction of a mandatory data breach notification law.

AISA notes that, if the proposed legislation is to have the intended effect of improving the security posture of Australian organisations, information about the reported data breaches should be made publicly available. The publication of data breach notification information is also important for a better understanding of the Australian data breach landscape and the sectors that may be most affected as well as the identification of any systemic issues.

**Recommendations**

- **AISA support the passage of the proposed legislation, subject to further clarifications discussed below.**

- **AISA recommends that consideration be given to further regulatory measures to encourage improved practices in relation to network and data security. AISA would be pleased to engage with government and other relevant stakeholders in regard to the consideration of such regulatory measures.**

- **AISA supports the annual publication by the Privacy Commissioner of details of data breach notifications, suitably anonymised where relevant. The publication of such information is important for a better understanding of the Australian data breach landscape, the sectors that may be most affected and the identification of any systemic issues.**

**3.2. Notification Threshold**

The 2016 AISA member survey posed a number of questions in regard to the proposed notification threshold, which is, where there are reasonable grounds to believe that there is ‘real risk of serious harm.’

Respondents were asked whether they thought the “real risk of serious harm” to the data subject was the right threshold for notification. Nearly 60% of respondents answered ‘no’ while 30% answered ‘yes’ and 10% believed they could not say.

---

5 2016 Survey, Question 1.
Although this result may suggest that a large majority do not believe the threshold is appropriate, it is not clear why respondents were of this view. Results from previous surveys would suggest that members regard this threshold as too high,\(^6\) however there may also be concerns relating to the ability to interpret and apply the threshold proposed.

AISA members were asked whether “reasonable grounds to believe” that there was a real risk of serious harm was too low a threshold for notification.\(^7\) Nearly 62% of respondents were of the view that the threshold was too high, with 30% believing it is too low. This is consistent with previous findings to the effect that a majority of members are in favour of a lower notification threshold.\(^8\) A small majority from the 2012 survey preferred that notification be triggered where there has been a material breach of data security safeguards which may create a reasonable risk of serious harm, with 33.3% of respondents supporting notification of any data breach, unless there is no reasonable risk that the breach will result in any harm.

AISA believes that its members are still uncertain as to the preferred notification threshold. Given this uncertainty, AISA proposes that the operation of the legislation be reviewed after 24 months to assess how effectively it is operating, having regard to the intended outcomes from the passage of the Bill.

**Recommendations**

- *AISA members would prefer a lower threshold notification than where there are reasonable grounds to believe there is a ‘real risk of serious harm.’*

- *In any case, AISA recommends that the operation of the legislation be reviewed after 24 months to assess how effectively it is operating.*

A series of questions were asked about AISA members’ ability to assess whether this threshold had been met.

---


\(^7\) 2016 Survey, Question 8.

\(^8\) See AISA DBN Submission 23 November 2012, Recommendation 2.1, page 16. Less than 5% of respondents were in favour of the proposed ‘real risk of serious harm’, with the balance supporting a range of lower notification thresholds.
3.3. **Real risk of serious harm.**

Members were asked about their ability to tell whether serious harm was likely to result from a data breach. Members were divided: 45% thought it was unlikely while the balance thought it either possible (42.75%) or likely (12.25%) that they would be able to tell.

Members were asked whether, when applying the threshold of ‘real risk of serious harm’ they would know how to make that assessment.⁹

52% of participants said ‘no’ and 17% ‘couldn’t say.’ Effectively **69.4%** of respondents (more than 95 people of the 138) stated that they could not or did not know if they could assess if there is “real risk”.

To help clarify how the assessment is to be made by the different stakeholders who may participate in that process, specific guidance could be provided. The provision of such guidance is recognised as an important part of the regulatory dialogue that needs to be in place to support a shared and well defined understanding of any principles-based regulatory system.

To support this regulatory dialogue, AISA suggests that the Privacy Commissioner consider establishing an expert advisory panel representing relevant stakeholders, including the information security community, to work with the Commissioner on identifying areas for clarification and developing relevant guidance and clarification.

**Recommendation**

- **AISA recommends further clarification be provided as to the assessment of whether there is “real risk”.** For example, notification might be required where harm is ‘possible’ to any of data subjects whose information has been compromised.

- **AISA recommends that additional guidance be provided to assist in the assessment of whether there is a real risk of serious harm.**

---

⁹ 2016 Survey, Question 3.
AISA recommends that the Privacy Commissioner establish an expert advisory panel representing relevant stakeholders, including the information security community, to work with the Commissioner on identifying areas for clarification and developing relevant guidance and clarification.

3.4. Loss Likely to lead to access or disclosure

AISA members were asked whether they would be able to assess whether a data loss was likely to lead to unauthorised access or disclosure\(^\text{10}\) and whether they thought that this provision was setting the bar too low.\(^\text{11}\) Although members were divided as to whether or not they would be able to assess the likelihood of unauthorised access or disclosure where data is lost, 60% of respondents were happy that the bar as set either too high or just right.

Recommendation

- **AISA recommends that additional guidance be provided to assist in the assessment of whether a loss is likely to lead to unauthorised access or disclosure.**

3.5. Harm

In response to the question whether respondents would be able to tell whether **serious harm** was likely to result from a data breach,\(^\text{12}\) the answers were divided: Approximately 45% believed they would be unlikely to make this assessment, while 55% were of the view that such an assessment was possible or likely.

Respondents were asked about their confidence in their ability to assess “serious harm” when “harm” is defined to include “physical harm, psychological harm, emotional harm, harm to reputation, economic harm and financial harm.”\(^\text{13}\)

Respondents were also asked whether they would support deleting “emotional” and “psychological” harm from the list of possible serious harms.\(^\text{14}\) Over 50% of

---

\(^{10}\) 2016 Survey, Question 4.

\(^{11}\) 2016 Survey, Question 5.

\(^{12}\) 2016 Survey, Question 2.

\(^{13}\) 2016 Survey, Question 6.

\(^{14}\) 2016 Survey, Question 7.
respondents were not in favour of deleting these reference. Accordingly, AISA considers that emotional and psychological harm should remain in the Bill but be made objective by making them subject to a reasonableness test.

**Recommendation**

- **AISA recommends that emotional and psychological harm be defined by reference to a reasonableness test.**

**3.6. Reasonable grounds to believe**

AISA members were asked whether “reasonable grounds to believe” that an organisation has suffered a serious data breach was too low a threshold for notification. Over 62% of respondents regarded this as an appropriate threshold. Accordingly, no recommendations are made in this regard.

**3.7. Risk Mitigation**

Members were asked whether they supported an exemption from the reporting requirements where the loss or risk of loss to the individual has been mitigated.

On balance AISA members believe that notification should be required even where it is possible to otherwise mitigate the risk of loss flowing from the data breach. Accordingly, no recommendations are made in this regard.

**3.8. Encryption**

Members are divided on whether there should be a specific exemption for a data breach affecting encrypted information. They were asked whether the law should make it clear that loss of encrypted information is not subject to the notification rule even if it contains personal information. 44% of respondents thought that there should be a specific exception while over 46% were of the view that there should not be. Given this divided view, AISA recommends that issues such as encryption be covered by additional guidance, developed in consultation with the expert advisory panel. AISA would be

---

15 2016 Survey, Question 8.
16 2016 Survey, Question 11.
17 2016 Survey, Question 14.
delighted to provide a nominee to participate in any expert panel or other assist in developing guidance relevant to security controls.

**Recommendation**

- AISA support the existing approach to the issue of encrypted data and recommends that issues such as encryption be covered by additional guidance, developed in consultation with the expert advisory panel.

### 3.9. Obligation to notify where an Overseas recipient suffers a data breach

The survey results indicate concern regarding the ability to notify when an overseas recipient has suffered a relevant data breach. This concern is understood to be related to the existence of contractual arrangements and the systems and procedures necessary to ensure compliance with this obligation. Accordingly, we request that this requirement be subject to a longer sunrise period, where the overseas organisation is not otherwise subject to any notification obligations.

**Recommendation**

- AISA recommends that the sunrise period for mandatory data breach notification to apply to information held by overseas recipients be increased to 3 years, for third parties not otherwise subject to any notification obligations, so that organisations have time to review and renegotiate the contractual arrangements necessary to ensure that they will have the information and investigatory powers necessary to ensure compliance.

### 3.10. Single Notification Mechanism

Members were asked whether they would support a mechanism to prevent multiple parties for having to notify the same individuals about the same breach.\(^\text{18}\)

At 81.8%, the overwhelming majority of respondents are in favour of an EU type approach that would allow for one party to notify the same customers rather than having

\(^{18}\) Question 12.
multiple parties, all of which might be regarded as ‘holding’ the information, notify the same individuals about the same breach.

**Recommendation**

- *AISA recommends the introduction of an EU type “data controller/processor” distinction where the processor only has an obligation to report to the controller and the controller has the responsibility to report.*
Appendix A: AISA DBN Questionnaire

The AISA survey questionnaire was released on 17 February 2016 and included a total number of 16 questions (shown in the table below). A total of 138 responses were received from AISA members.

<table>
<thead>
<tr>
<th>ID</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Do you think the proposed threshold for mandatory data notification being “real risk of serious harm” to the data subject is the right threshold?</td>
</tr>
<tr>
<td>2</td>
<td>When a data breach occurs is it unlikely, possible or likely that you will be able to tell whether serious harm is likely to result?</td>
</tr>
<tr>
<td>3</td>
<td>In applying this threshold, do you know how to assess whether or not there is a “real risk” of serious harm?</td>
</tr>
<tr>
<td>4</td>
<td>In your experience, if data is lost are you usually able to assess the likelihood that there will be unauthorised access or disclosure?</td>
</tr>
<tr>
<td>5</td>
<td>Where data is lost does the fact that you will have to notify if unauthorised disclosure of, the information is likely to occur, set the bar too low?</td>
</tr>
<tr>
<td>6</td>
<td>Are you confident in an ability to assess “serious harm” when “harm” is defined to include “physical harm, psychological harm, emotional harm, harm to reputation, economic harm and financial harm”?</td>
</tr>
<tr>
<td>7</td>
<td>Would you support having “emotional” and “psychological” harm deleted from the list of possible serious harms</td>
</tr>
<tr>
<td>8</td>
<td>The new law requires you to notify the privacy commissioner and the data subject of the breach if you are aware or have “reasonable grounds to believe” that your organisation has suffered a serious data breach. Is “reasonable grounds to believe” too low a threshold for notification in your view?</td>
</tr>
<tr>
<td>9</td>
<td>The proposed law provides that you can take 30 days to investigate and make a call on notification if you become aware or have reasonable grounds to believe that your organisation has suffered a serious data breach. Is this enough time?</td>
</tr>
<tr>
<td></td>
<td>Question</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>10</td>
<td>The proposed law will require data breach notification where your organisation has disclosed information to an overseas recipient and the recipient has suffered unauthorised access and disclosure with a “real risk of serious harm”. Will you be able to comply with this obligation?</td>
</tr>
<tr>
<td>11</td>
<td>Do you think it would be reasonable to be exempted from the reporting requirements if the loss or risk of loss to the individual has been mitigated?</td>
</tr>
<tr>
<td>12</td>
<td>Would you support a mechanism to prevent multiple parties for having to notify the same individuals about the same breach: i.e. would you support a EU type “data controller/processor” distinction where the processor only has an obligation to report to the controller and the controller has the responsibility to report.</td>
</tr>
<tr>
<td>13</td>
<td>Should the law allow for parties involved in a service to agree amongst them who must report and when that has happened it should be the responsibility to report can be discharged by the party so contracted.</td>
</tr>
<tr>
<td>14</td>
<td>Should the law should make it clear that loss of encrypted information is not subject to the rule even if it contains personal information?</td>
</tr>
<tr>
<td>15</td>
<td>Do you think a mandatory data breach notification law will result in improved network and data security?</td>
</tr>
<tr>
<td>16</td>
<td>Will a mandatory data breach notification law make your job easier or more difficult?</td>
</tr>
</tbody>
</table>

Table 1: AISA Questionnaire