GPO Box 4052,
Sydney, NSW 2001

icare.nsw.gov.au

Consultation Paper on Mandatory Notification of Data Breaches by NSW Public Sector Agencies – icare submission

icare is supportive of mandatory notification of serious privacy breaches provided there are clear and concise definitions and guidelines set down by the NSW Privacy Commissioner on the types of breaches that need to be notified, the actions required to be taken and consequences.

Questions

1. **Should the NSW Government introduce a mandatory data breach notification scheme forNSW public sector agencies?**

   If mandatory notification of privacy breaches is implemented, icare's view is that it should be limited to serious breaches (which should be defined) and that the scope and implementation are appropriate in the lightof the potential administrative burden. In this regard, the setting of realistic time-frames, clear and concise definitions and manageable obligations are essential.

   In general, icare supports the introduction of a mandatory scheme for the following reasons:

   - Removes current voluntary obligations;
   - generates a focus on data breaches;
   - aligns with federal privacy laws; and
   - meets community expectations.

2. **Should legislation require NSW public sector agencies to report breaches:**

   a) **Where unauthorised access to or disclosure of personal information has occurred?**

   To the extent that mandatory notification of breaches is introduced, icare is of the view that this should be limited to situations where a data breach is likely to result in serious harm to an individual whose personal information is involved and the agency has not been able to prevent the likely risk of serious harm with remedial action. A data breach occurs when personal information an agency holds is lost or subjected to unauthorised access or disclosure.

b) Where any breach of an Information Protection Principle has occurred?

icare considers that making a breach of the Information Protection Principles subject to mandatory notification would impose an unacceptable administrative burden on agencies such as icare and on the NSW Privacy Commissioner.

The principles are replete with concepts such as 'such steps as are reasonable in the circumstances', 'not excessive' and 'an unreasonable extent'. Reasonable minds may differ as to the interpretation of these concepts.

Additionally, little interpretive assistance is provided by cases considering the principles as many of them are tribunal decisions that rely on specific facts.

3.

a) Is the threshold of 'likely to result in serious harm' appropriate, or should a different standard be applied?

See answer 2(a) above.

b) Should legislation define the term 'serious harm'?

Yes, the clarity and certainty of legislative guidance is desirable. Consistency with the Commonwealth NDB scheme would likewise be desirable. Especially to the extent of the definition of 'serious harm' as they may be challenging to reach due to the variability of a breach and the potential harm it could cause to individuals. It is noted that different topics to consider (financial, reputational, physical, etc) are useful for agencies to factor in their assessments. Where possible, associating examples or methods to calculate serious harm will assist agencies in determining whether its breach constitutes 'serious harm'.

c) Should legislation prescribe the factors an agency must consider when assessing whether a data breach meets the threshold of serious harm?

Yes, provided that such factors are clear and unambiguous and that the list is inclusive, rather than exhaustive. icare supports these prescribed factors aligning with those in the Commonwealth NDB scheme to assist with consistency, clarify and certainty.

4. Should legislation require NSW public sector agencies to report data breaches only where the agency has been unable to prevent likely risk of serious harm with remedial action?

Yes, this approach would minimise unnecessary distress to the relevant individual. It would also reduce the administrative burden on agencies such as icare and align with the Commonwealth NDB scheme.

There is benefit in only needing to report once the potential of serious harm has been assessed, and the remedial action has not reduced the harm to an acceptable level. There is a risk of overreporting if a proper triaging process does not occur.

5.

a) What information should be notified to the NSW Privacy Commissioner and affected individuals in relation to data breaches?

The legislation should create a distinction between notification of the NSW Privacy Commissioner and the individual. The former should receive information as per cl 4.18 of the consultation paper, with an exemption for information that is not readily available in the light of an agency's limited resources. The latter should receive similar information, but in plain English, and with a focus on remedial action that the individual may take and that the agency is taking.

Additionally, the legislation should permit the agency to consider the safety of any individual when framing the content of a notification. Where the notification to an individual may cause harm or be detrimental to the individual (for example, on medical grounds or mental health grounds) notification should not be required. The legislation can set out clear definitions on when an exception would apply. Furthermore, in cases where an agency conducts its assessment and is of the view that certain people whose personal information was involved in the breach are not likely to suffer serious harm, then there should be no requirement to notify those particular individuals.

Consideration is being given to the notifications to the Privacy Commissioner to include "the estimated costs of the breach to the agency". If this information is agreed to form part of the notification to the Privacy Commissioner, it should only be anticipated to be supplied at the conclusion of the data breach investigation, when the assessment of estimated cost can be reliably made, and any such information provided to the Privacy Commissioner should be the subject of confidentiality due to the commercial in confidence nature of the information. There is also the factor to be considered that should the affected party decided to pursue the matter through the NSW Civil and Administrative Tribunal where potential costs can be awarded against an agency for a maximum of $40,000 post data breach notification.

b) Should the legislation prescribe the form and content of the notification?

In relation to form:
Yes, provided that the prescribed form accommodates the differing technologies available to agencies.

In relation to content:
Yes, provided that the legislation aligns with answer 5(a) above, does not impose an excessive administrative burden and is clear and unambiguous.

6. What notification timeframe should be prescribed in the legislation?

A distinction should be made between breaches that may lead to possible serious harm to an individual and/or involve potentially criminal conduct and those of a less serious nature. The former should be notified as soon as is practicable, or not later than 30 days (in line with the Commonwealth NDB scheme).

All other breaches should be notified within 60 days (unless there are extenuating circumstances), in line with notification requirements of internal reviews. icare submits that this is a realistic time-frame, given the quantity of information and complexity of the storage systems that such agencies use.

In particular:
icare estimates it currently manages (88, 000) claims on behalf of the Nominal Insurer, the NSW Self-Insurance Corporation and a number of other schemes.

It is worth noting that icare has been voluntarily notifying the NSW Privacy Commissioner of serious data breaches in relation to these claims since January 2016.

icare is concerned that if there is insufficient time allowed for the provision of a notice, the resultant hasty decisions may lead to undesirable consequences. Are the timeframes going to be legislated or will they be at the discretion of the Privacy Commissioner or will the agency be granted discretionary powers depending of the situation of the data breach ie malicious attack forensic analysis taking longer than anticipated.

7.

a) Does the NSW Privacy Commissioner require any additional powers to encourage compliance with a mandatory notification scheme?

The Privacy Commissioner already has expansive powers under s36 of the Privacy and Personal Information Protection Act 1998, which could ensure that agencies will take the introduction of the scheme seriously. The Privacy Commissioner could use the powers that may be necessary in the event that an agency is failing to provide a suitable response.

b) Should monetary penalties apply where NSW public sector agencies fail to comply with the requirements of the scheme?

icare does not believe the monetary fines will be effective as the IPC is regulating other NSW government entities. Any fines are paid for out of the NSW Government monies. The scheme should contemplate other regulatory tools such as mandatory publication of breaches and non-compliance.

8. What exemptions from the requirement to notify individuals and the NSW Privacy Commissioner of eligible data breaches should apply?

Exemptions may apply if the agency believes that the notification of the breach to an affected individual may adversely impact the individual, for example if the individual is at risk of harming themselves. However, in that instance, the scheme should still require the agency to notify the Commissioner.