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)*	**Insurance Brokers - Cyber Data-Risk Managers Pty** Contact Person: ***Meena Wahi***
Contact details *(one or all of the following: postal address, email address or phone number)*	**Email:** info@dataprivacyinsurance.com.au **Ph.No:** 02 89871913

Confidentiality

Would you prefer this submission to remain confidential? YES / **NO**

SUBMISSION

Response to the consultation paper on **regulation impact – of three options** and specifically for option of 'mandatory notification'.

Cyber Data-Risk Managers, specialist insurance brokers for cyber and data privacy risk would like to argue in favour of mandatory notification as the best option outlined in the consultation paper.

How will Mandatory Notification help?

Mandatory notification if it becomes a regulatory obligation- would impose specific response on part of business that experiences a data breach - to make public the data breach & to inform individuals whose privacy has been breached as a result of the incident. Notification would reveal unknown or hidden risks inherent in the business operations including security vulnerabilities & threats. Reputational risk would motivate the business to eliminate underlying cause to mitigate further loss to the business.

Risk Management
Cyber and privacy risk is less evident and less insurable in voluntary notification scenario. As data breach incidents increase, Insurers are unlikely to accept a simple transfer of risk – they would expect businesses to disclose all past data breaches and investment in security. Mandatory notification would make it easier for businesses to declare past incidents of data breach in their application for insurance – to facilitate a genuine assessment of the risk that they wish to transfer to the Insurer. A fair premium price shall result with the Insurer more confident of possessing all facts and more willing to insure the risk.

Cost of Mandatory Notification

Introduction of mandatory notification would increase the cost of regulatory liability for businesses. The cost of mandatory notification for a business would comprise of cost of notification & public advertisements; cost of reputational loss –including loss of trust, customer retention, brand image and perception in the community plus unplanned crisis response costs.

Cyber insurance as an insurance for ***Crisis Response, Indemnity and Liability.***

Cyber insurance as an insurance offsets the costs associated with crisis response, indemnity and liability related to a cyber incident. Cyber insurance triggers when a cyber or data privacy breach is reported by the insured. For a business to claim for costs associated with a data breach/cyber attack – the loss must be directly associated with the incident.

Insurance coverage (*coverage differs depending on the insurance policy*)

Crisis Response: Cost of notification, PR expense, Credit monitoring costs for identify theft

Indemnity: Restoration of data/digital assets to original state & coverage for costs business would not have incurred had the breach / cyber incident not happened.

Liability: Costs incurred for regulatory response as part of regulatory obligation to submit breach report. Payout of fines imposed by Regulator. Legal defence fees & legal payouts