THE NOTIFIABLE DATA BREACHES SCHEME – CYBER INSURANCE.
by Gregory Ross |

The **Privacy Amendment (Notifiable Data Breaches) Act 2017** established the Notifiable Data Breaches (NDB) scheme in Australia but I query issues to do with cyber insurance. The laws commenced 22 February 2018. I don't here address the detail of the operation of the provisions, but ask some questions about when things go wrong, particularly, I raise the need for cyber insurance.

NDB Scheme

The NDB scheme applies to all agencies and organisations with existing personal information security obligations under the Australian Privacy Act 1988 (Privacy Act) to require action to secure certain categories of personal information. This includes Australian Government agencies, businesses and not-for-profit organisations with an annual turnover of $3 million or more, credit reporting bodies, health service providers, and TFN recipients, among others.

The NDB Scheme mandates notification to individuals whose personal information is involved in a data breach where that disclosure is likely to result in serious harm. The notification must include recommendations on the steps individuals should take in response to the breach.

The breach must also be notified to the Australian Information Commissioner.

There is a Notifiable Data Breach statement form.

Agencies and organisations must be prepared to conduct a quick assessment of a suspected data breach to determine whether it is likely to result in serious harm, and as a result require notification.

"Serious harm" is not, I believe, defined adequately. The OAIC site includes comments such as:-

It involves a fairly prompt decision on whether an "eligible data breach" has occurred and "whether, from the perspective of a reasonable person, the data breach would be likely to result in serious harm to an individual whose personal information was part of the data breach". — "The phrase 'likely to occur' means the risk of serious harm to an individual is more probable than not (rather than possible)."

The OIC website talks in terms of "In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm."

Which data breaches require notification?

The scheme applies to data breaches involving personal information that are likely to result in serious harm to any individual affected but the legislation is of little help. The OAIC website suggests there are exceptions but I have yet to find any useful definition.

Assessing suspected data breaches

Personal information holders that suspect an eligible data breach may have occurred must undertake a reasonable and expeditious assessment to determine if the data breach is likely to result in serious harm to any individual affected. Where so determined, it must be relevantly notified.

The Cost and Who Covers It

Where there is a relevant breach, the question arises, how to bear the cost of compliance and any loss. Some of those costs will be internal, some will be external.

The NDB Scheme is in its early days and obviously different businesses will have varying degrees of exposure and they and their clients will suffer different types and amounts of loss where a relevant data breach occurs.

In my view, the implications of the NDB Scheme for most businesses holding "personal information" include what might best be described as check, polish and refinement of existing systems and procedures, rather than major change.

For some clients I have prepared a checklist of things to review and how they can best be addressed and or remediated to ensure compliance. Some of the improvements are as simple as better use of passwords.

However, one can't deny the prospect that someday a relevant data breach will occur so triggering the operation of the NDB Scheme. Where that happens, there is real potential for significant cost and possibly large loss.

I have had occasion to peruse a few insurance offerings expressed to deal with the exposure of businesses affected by the NDB Scheme.

Granted the area of cover is relatively new, but the wording of policies I have seen seem to have more than a few too many loopholes. They are usually broader than just to cover NDB Scheme exposure.

Issues on Respect of Cover and Policy Wording

The list of issues to be aware of in considering obtaining cover includes:-

1.There is an unclear line between "professional responsibility" cover relevant to particular businesses and "cyber cover" as concerns cyber issues and loss of data, which could range from hacking to a lost device, especially of the type covered by the NDB Scheme;
2. With most "business" policies not clearly extending to and often excluding cyber and computer issues a number of policies have hit the market. They can deal with issues like protecting business against a number of different cyber attacks or events, including cover for:-

- System Damage: For rectification costs in repairing, retrieving, replacing or restoring computer records or computer records a business is responsible for that have been hacked, destroyed, damaged or lost due to a cyber event.
- Computer Virus And Hacking: Cover for claims and defence costs as a result of a third party's financial loss due to a hacking attack or virus that began or passed through a business' computer systems.
- Extortion Cover: For cyber extortion costs incurred in responding to a security threat to a computer systems. Cover includes extortion payments and costs involved in negotiating, mediating and crisis managing to end the security threat.
- Privacy Fines & Investigations: For fines or penalties payable by a business (to the extent permitted by law) as a direct result of a breach

of a business's privacy obligations. Cover can include regulatory investigation costs into the breach.

- Privacy Breach Notification & Loss Mitigation: For privacy breach costs incurred as a direct result of a cyber-attack or event. Cover includes paying the costs of establishing a credit monitoring service or identity theft helpline or providing call centre support services.
- Privacy Breach: Cover for claims and defence costs in the event of a breach of: a person's privacy, a company's commercially confidential information, employee's privacy.

3. policies may, not surprisingly, require consistency of patches of operating systems in accordance with vendor updates and the like, so requiring a degree of ongoing self management of the issue in a risk reduction sense by the insured;

4. installation and maintenance of proper latest antivirus programs may be required;

5. ongoing training of staff seems an imperative, particularly in respect of potentially malicious email;

6. one policy included a cyber notification and claims protocol and procedure, though I'm not sure how well tailored that is to the Australian context, particularly about creation of mitigation response plans which may require "client" consent and involvement, depending upon circumstances. Would that have to be sent out, for instance, in a professional's terms of engagement with clients?

7. Whether the policy extends only to systems owned and/or leased by the business and any dependent business and not to personally owned devices of any of its staff are used in connection with business operations.

The text of the paper is only a summary and discussion of particular facts and principles. It is not to be taken as legal or commercial advice as to any particular factual circumstances but feel free to contact the writer if you have any queries or comments.