Cyber checklists

BREACH RESPONSE

wotton kearney

A founding member of LEGALIGN GLOBAL

Guide to Cyber Breaches

Responding to cyber breaches is a comprehensive process, but the three key elements are:

Step 1: Follow your incident response plan

Step 2: Notify your insurer

Step 3: Comply with your legal obligations

The below chart provides a basic framework for responding to a cyber breach.

Step 1: Follow your incident response plan

Immediately following a cyber breach, the key focus should be to contain the breach and remove the attacker from your systems. Your incident response plan (as outlined in our cyber readiness guide **here**) should provide a clear process for this and the personnel in charge of each step.

Step 2: Notify your insurer

As part of your incident response plan, you should notify your insurer and get their advice on incident management. This will often involve obtaining legal representation to assist you in responding to the incident and engaging third party experts such as forensic IT providers, to stop the breach.

Notifying your insurer early in the breach process will additionally assist you if you need to make a later claim for restoration costs, business interruption costs or third-party losses, as they will be able to track your losses and expenditure across the entirety of the incident.

Step 3: Comply with your legal obligations

This is the most intricate step in responding to a data breach is complying with your legal obligations under the Privacy Act and Notifiable Data Beach Scheme (NDB scheme). To understand your legal obligations, refer to our guides on the **NDB Scheme** and **Cyber Readiness**.

If you have no obligations under the NDB Scheme, you aren't required to notify your customers/ clients or the OAIC about the breach. However, you may consider making a voluntary notification.

If you are covered by the NDB Scheme you need to form a view, perhaps with the assistance of legal advice, as to whether you've suffered an eligible data breach. An eligible data breach occurs when:

1. there is unauthorised access to, unauthorised disclosure of, or loss of information where it is likely to be accessed or disclosed; which
2. a reasonable person would conclude would likely result in serious harm to any of the individuals to whom the information relates; and
3. you are unable to take remedial action to prevent the risk of serious harm.

If, following a cyber incident, you have reasonable grounds to suspect a data breach may have occurred but are unsure whether the relevant circumstances meet the criteria, you have 30 days to investigate the breach and make a reasonable assessment about whether it was an eligible data breach. You will need to identify, as far as possible, what information was accessed during the breach and which individuals were affected. Forensic IT providers will be able to help you with this assessment process

If, during that investigation, you have reasonable grounds to believe that a cyber incident amounts to an eligible data breach, you must notify the Office of the Australian Information Commissioner (OAIC) and affected individuals as soon as possible.

If notification is required, the Privacy Act requires a statement to be prepared that at the very least includes:

1. your organisations or agency's name and contact details;
2. a description of the data breach;
3. the kinds of information involved; and
4. recommendations about the steps individuals should take in response to the data breach.