



## A guide to developing your data breach response plan



**Gallagher**

Insurance | Risk Management | Consulting

# Contents

**Complacency will cost you**.....3

    A data breach response plan:  
    what it is, and why you need one.....3

    What to expect in this guide .....3

**Getting started**.....4

    Medium to large businesses .....4

        Assemble your data breach response team

        Example response team structure

        When should the response team be activated?

    Small to medium sized enterprises.....5

        Get help from the experts

        Purchase the right insurance

        Start putting together a plan

**Example data breach response plan checklist**.....6

**About Gallagher**.....7





# Complacency will cost you

According to research published by [IBM and Ponemon Institute](#),<sup>1</sup> **the average Australian data breach in 2018 saw 19,442 records exposed or compromised**. The average cost of these breaches to an Australian organisation was **\$1.99 million**. The research also found that the average global probability of a material breach over the next 2 years stands at **27.9%** – a 2.2% increase from 2017.

So the bottom line is that data breaches are expensive, and they're increasingly common. **It's no longer a question of if your company will be breached, but when.** So how will your organisation respond?

## A data breach response plan: what it is, and why you need one

A data breach response plan is a tool for managing and mitigating the impact of a data breach. Think of it as framework for organising your response efforts; it sets out the roles and responsibilities for people within your organisation tasked with managing a breach.

There are several reasons why you need a data breach response plan:

### 1. **It will help you meet your obligations under the *Privacy Act***

As a company, you're obligated to take [reasonable steps](#) to protect any personal information from misuse, interference and loss as well as unauthorised access. Those 'reasonable steps' likely include having a data breach response plan.

### 2. **The Notifiable Data Breaches (NDB) scheme commenced on 22 February 2018**

This [scheme](#) requires organisations to notify individuals if they've been affected by a serious data breach. Having a data breach response plan will make it easier to adhere to the NDB scheme and avoid fines for noncompliance.

### 3. **It helps protect your assets**

A data breach results in the loss or exposure of your company's most important asset – its data. But it can also result in substantial reputation damage, fines, legal bills and loss of future profitability. A data breach response plan will help you mitigate the impact of a data breach and stop additional loss, while also maintaining a high standard of customer service and transparency.

## What to expect in this guide

In this guide we'll show you **how to develop your data breach response plan**, with advice and tips for best practices along the way. You'll also find an **example response task checklist** that you can use as the basis for your plan, as well as other helpful resources.

Remember: every organisation is different. The information in this guide is general and you can adapt it for your organisation's needs. If you have any questions or would like more information, get in touch with our specialist cyber risk team.



<sup>1</sup> IBM/Ponemon Institute (2018) 2018 Cost of a Data Breach Study: Global Overview

# Getting started

A written data breach response plan is just one piece of the puzzle. There are a few things you need to do before you get to that stage.

## Medium to large businesses

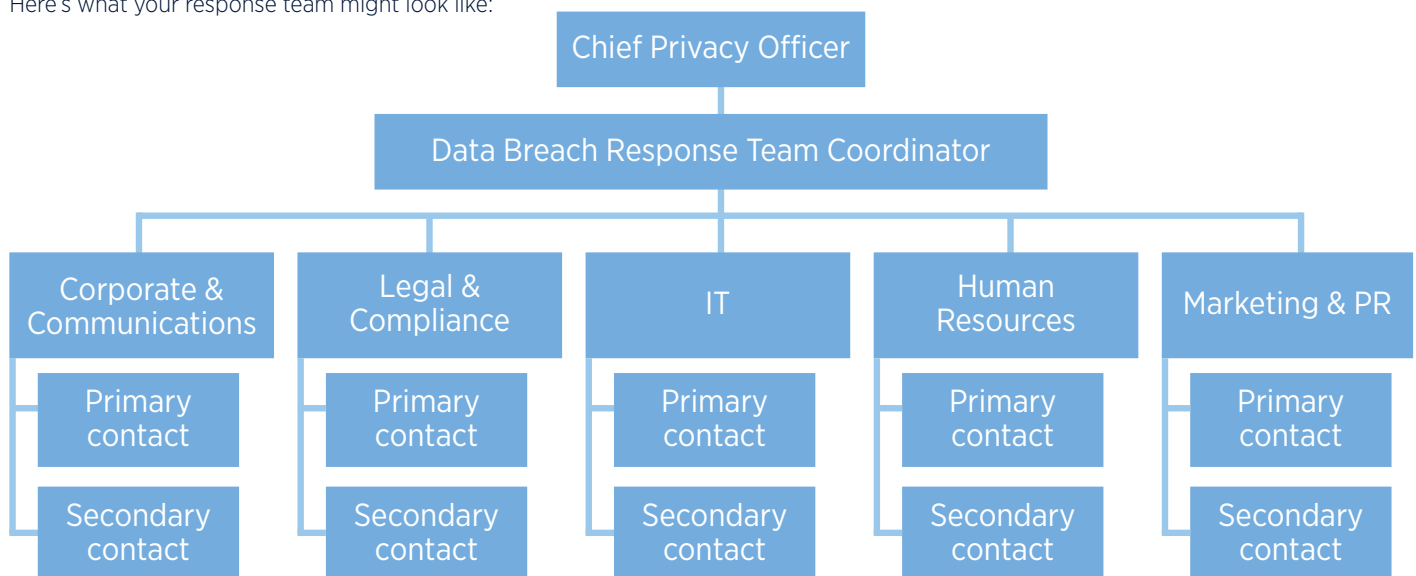
### Assemble your Data Breach Response Team

Your Data Breach Response Team ('response team') is responsible for coordinating your company's response efforts in the event of a breach. They play a critical role in mitigating the damage caused by a breach and execute your data breach response plan.

The response team needs to be aware of its responsibilities and activated the moment a breach is discovered, so it's important to have them **assembled and trained** in advance.

#### Example response team structure

Here's what your response team might look like:



#### When should the response team be activated?

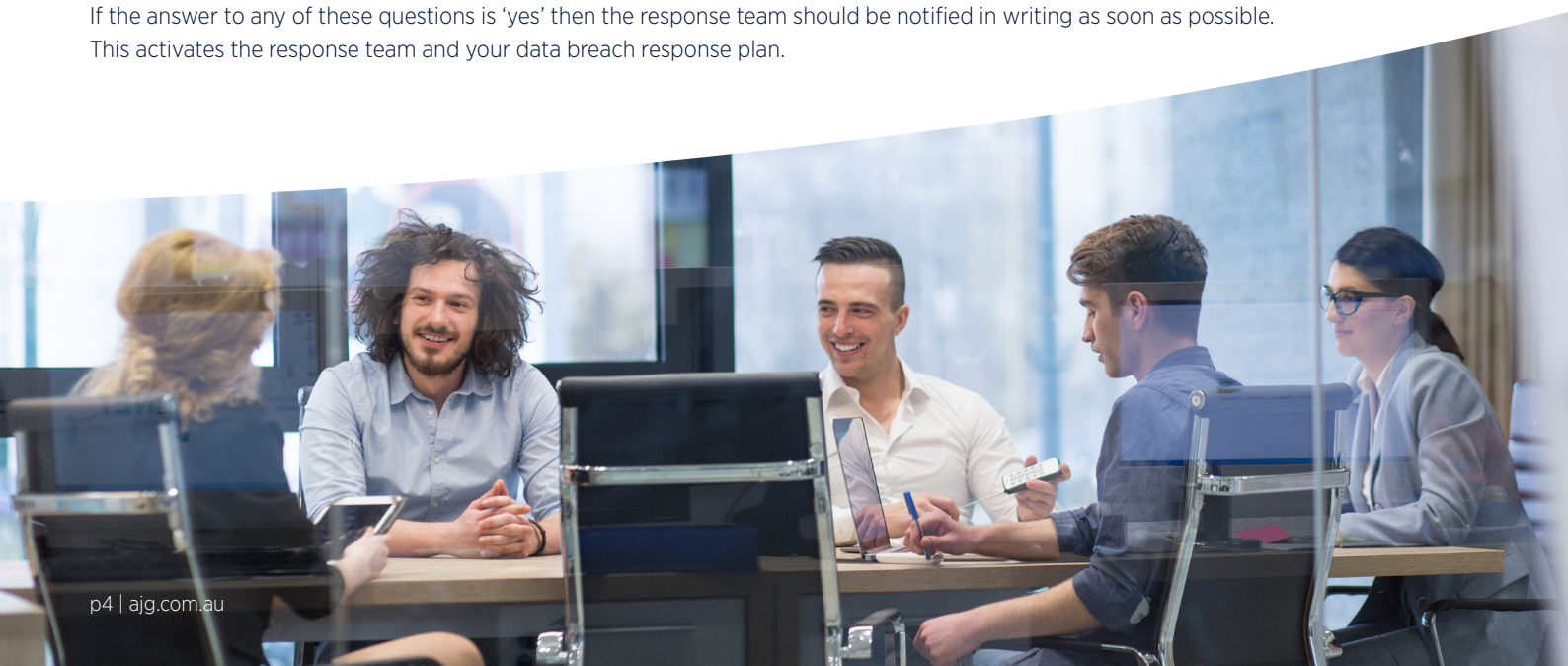
Not all data breaches require a formal response, and it is the CPO or director's job to determine whether a breach needs to be escalated to the response team and reported to the [Office of the Australian Information Commissioner \(OAIC\)](#) and individuals whose data is affected, in compliance with [mandatory requirements](#).

But how do they decide whether a breach should be escalated? Consider these questions:

- How many individuals, if any, have been affected by the breach? Is there a risk of significant harm to these individuals?
- Was the breach caused by a breakdown in company process, procedure or security protocol?
- Could there be legal, financial or reputational ramifications?

If the answer to any of these questions is 'yes' then the response team should be notified in writing as soon as possible.

This activates the response team and your data breach response plan.



## Small to medium sized enterprises

Small to medium enterprises (SMEs) with less than 200 staff represent 96 per cent of Australian businesses, and employ almost half of Australia's private workforce.

According to a 2018 cyber security report by [Deakin University](#), 60% or 42,000 of the annual 700,000 cyber attacks on Australian businesses target SMEs.

### The report recommends seven simple steps for SMEs to protect themselves.

1. Patch systems and enable automatic patching. All systems and packages are updated (called patching) and the patching can be done automatically rather than implemented individually by users.
2. Back up all important data.
3. Use a cloud based email and/or data storage.
4. Use strong authentication. Use passphrases instead of passwords and use two-stage authentication where possible.
5. Set up different accounts. For example you can set up an administrator account, as well as user accounts.
6. Don't use the same password across all accounts. When one is hacked, they all become vulnerable if you're using the same password.
7. Don't click on links, attachments or images from people not known to you. Criminals often hack one account and use that account to send malware to people in the contact list.

### Your obligation if you think a data breach has occurred

If an organisation suspects a breach of data containing personal information has occurred it is required to record a detailed assessment within 30 days to both the [Office of the Australian Information Commissioner \(OAIC\)](#) and the individuals whose data is compromised whether this has in fact happened.



### Purchase the right insurance

Considering that data breaches are increasingly common (and a single data breach costs an average of \$1.99 million) it's important that you consider purchasing **cyber insurance**. Having the right coverage is essential for managing your cyber risk and protecting your business from significant financial loss in the event of a data breach.

Work with your **insurance broker** to develop an insurance program to cover risks such as:

- Financial loss arising from lost revenue, customer churn, privacy fines, court awards, legal expenses, forensic investigator costs and data reconstitution
- Reputation or brand damage
- Loss of intellectual property.

Your broker will also help you understand your risk exposures and your overall security posture, and they'll use this information to negotiate the terms and cost of your policy. They'll also help you decide whether you need additional coverage in the form of Directors and Officers' insurance or management liability insurance.

### Start putting together a plan

After assembling a response team and consulting with your insurance broker and external partners, you'll be well placed to start putting together your data breach response plan.

There is no single method or process for responding to a data breach. Your response depends on the nature and extent of the breach, the size of your company and other varying factors. At its core, your response plan should set out the **procedures** and **tasks** involved in assessing, mitigating and resolving the breach.

### Get help from the experts

It takes a village to mitigate the impact of a data breach. That's why it's important to proactively engage partners who can help you investigate, remedy and prevent security incidents. Consider engaging:

- **A forensics partner.** They can conduct in-depth technical investigations into data breaches, advise you on how to stop data loss and help you manage reporting and evidence gathering during an incident.
- **Legal counsel.** If you don't have the resources in house, an external legal partner is essential. They'll advise you on what you need to disclose to individuals and authorities and help you avoid litigation risks.
- **A communications partner.** Again, if you don't have the resources or capability in-house, it's worth investing in a communication partner to help you communicate with your customers and manage highly-publicised security incidents.

Don't wait for a data breach to happen before engaging partners; you don't want to rush the decision and commence a relationship with a firm you haven't fully vetted. Do your due diligence and be confident in your choice. After all, you'll be relying on them to help you through a very challenging time.

# Example data breach response plan checklist

Below is a **sample checklist of tasks** that a company with 500–1000 employees can use as the basis for a data breach response plan. You can adapt this checklist to suit your organisation's needs.

## CONTAINMENT



- ☐ **Record the date and the time the breach** is discovered. Also note down the date and time your response plan is activated.
- ☐ **Alert and activate the Response Team.** Begin executing the response plan.
- ☐ **Contain the breach.** Secure the area where the breach occurred and take affected machines offline.
  - ☐ Activate the ICT incident response plan.
- ☐ **Gather documentation.** Record who discovered the breach, to whom it was reported, the extent of the breach and any other evidence that may be of use to forensics firms and law enforcement.
  - ☐ Interview involved parties about their knowledge of the breach. Document their responses.

## EVALUATION



- ☐ **Launch initial investigation.** Begin collecting the following information:
  - ☐ Date, time, location and duration of breach
  - ☐ How the breach was discovered and by whom
  - ☐ Type of information compromised in the breach
  - ☐ What personally identifiable information (PII) or proprietary information was exposed, if any
  - ☐ Names of (possibly) affected individuals and organisations
- ☐ **Carry out a risk assessment.** Evaluate the extent of the damage caused by the breach to individuals and your business.
- ☐ **Assess priorities and evolving risks** based on what you currently know about the breach.
- ☐ **Engage a forensics firm.** Commence in-depth investigation into the breach.

## NOTIFICATION



- ☐ **Review notification procedures.** Determine who needs to be made aware of the breach, both externally and internally in preliminary stages. Ensure all notifications occur within mandated timeframes.
- ☐ **Notify affected individuals** if there is a real risk of serious harm. Where there is a high risk of serious harm, individuals must be notified immediately.
- ☐ **Notify law enforcement** if necessary, after consulting legal counsel and leadership.
- ☐ **Engage communications and PR teams.** Activate media plans and notification protocols.

## PREVENTION



- ☐ **Review findings of investigation into the breach.** Collate all documentation, evidence and findings for evaluation.
- ☐ **Update response plan** and other incident response plans as necessary.
- ☐ **Make appropriate changes** to policies and procedures, including information security and data management policies.
- ☐ **Revise staff training practices** to ensure staff have up-to-date knowledge of procedures and responsibilities.
- ☐ **Evaluate the response process** and audit if necessary.





### About Gallagher

Gallagher is one of Australia's – and the world's – largest insurance broking and risk management companies. We're the broker of choice for more than 120,000 Australian businesses – from micro-SMEs through to multinational corporations and iconic brands.

With 30+ regional and metropolitan branches across Australia, we understand local business communities because we're part of them ourselves.

Globally, the Gallagher network of 600+ offices in over 30 countries, enables us to leverage relationships with international insurance partners to create programs that achieve claims outcomes beyond the scope of many smaller brokers.





# Gallagher

Insurance | Risk Management | Consulting

Arthur J. Gallagher & Co (Aus) Limited. Operates under AFSL No. 238312. Any advice provided in this document does not consider your objectives, financial situation or needs. You should consider if the insurance is suitable for you and read the Product Disclosure Statement (PDS) and Financial Services Guide (FSG) before buying the insurance. If you purchase this insurance, we may charge you a fee for our service to you. Ask us for more details before we provide you with any services on this product. PDS available on request. Our FSG is available on our website, [www.ajg.com.au](http://www.ajg.com.au). Arthur J. Gallagher & Co (Aus) Limited. ABN 34 005 543 920, Level 12, 80 Pacific Highway, North Sydney, NSW 2060. REF1522-1118-3.2