Mandatory data breach reporting guide

Gallagher

Insurance | Risk Management | Consulting

REF001912-FEB18

Gallagher

Insurance | Risk Management | Consulting

From 22 February 2018 organisations subject to the *Privacy Act* (APP Entities) that hold personal information are required by law to report actual or suspected breaches of data security to the **Office of the Australian Information Commissioner** (OAIC) and to **the individuals whose data is compromised.**

Gallagher

Insurance | Risk Management | Consulting

Contacting the OAIC and individuals whose data is compromised

An outline of the Notifiable Data Breach notification scheme and **downloadable form** can be accessed via:

www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

Gallagher

Insurance | Risk Management | Consulting

What constitutes an eligible data breach?

Unauthorised access to or disclosure of personal information about one or more individuals where this could result in serious harm, including physical, psychological, emotional, economic, financial or reputational harm.

The **likelihood of harm occurring** is a factor, depending on the sensitivity of the information, whether it has been encrypted and how vulnerable such security measures might be to hacking.

Gallagher

Insurance | Risk Management | Consulting

Suspected breaches

If a suspected but unconfirmed data security breach has occurred **the organisation is required to record a detailed assessment** of whether this has in fact happened, within 30 days.

Gallagher

Insurance | Risk Management | Consulting

Penalties

Non-compliance with the Notifiable Data Breach scheme can attract penalties of up to **$1.8 million for businesses** and **$360,000 for individuals.**

The reputational damage from being publicly named is potentially even worse in terms of lost business.

Gallagher

Insurance | Risk Management | Consulting

What if the problem is remediated immediately?

An organisation's ability to **detect a data security breach and take immediate action to remedy it** is an important aspect of the likelihood of harm occurring, whether the breach is inadvertently caused by the organisation or its staff, or the deliberate action of a cyber criminal.

If the breach is effectively remediated it is not necessary to report it.

This is a compelling reason for having **dedicated cyber security resources and a coordinated plan** in case of a breach.

Gallagher

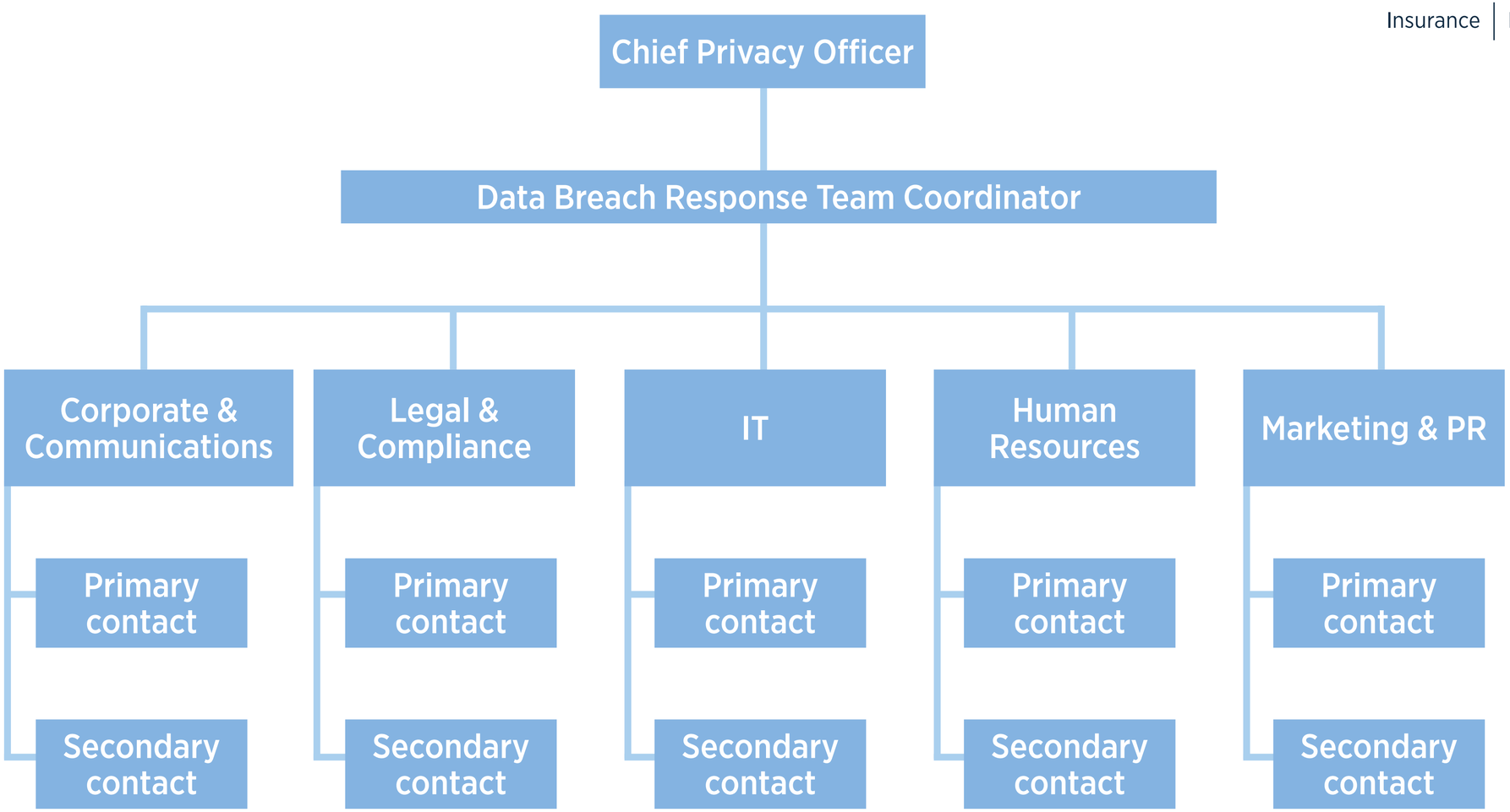
Insurance | Risk Management | Consulting

The need for a data breach response team

To respond quickly and effectively to a data breach your organisation needs a **dedicated team of trained personnel who can take immediate action.**

Gallagher

Insurance | Risk Management | Consulting



The information above is applicable to companies with between 500 – 1,000 employees but the advice is general and can be adapted to individual organisation's needs.

Gallagher

Insurance | Risk Management | Consulting

Sample data breach response plan checklist

Containment

Evaluation

Notification

Prevention

The information above is applicable to companies with between 500 – 1,000 employees but the advice is general and can be adapted to individual organisation's needs.

Gallagher

Insurance | Risk Management | Consulting

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.

Gallagher

Insurance | Risk Management | Consulting

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.

The information above is applicable to companies with between 500 – 1,000 employees but the advice is general and can be adapted to individual organisation's needs.

Gallagher

Insurance | Risk Management | Consulting

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.

The information above is applicable to companies with between 500 – 1,000 employees but the advice is general and can be adapted to individual organisation's needs.

Gallagher

Insurance | Risk Management | Consulting

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.

Gallagher

Insurance | Risk Management | Consulting

Forewarned is forearmed

All APP organisations should as a priority conduct an up-to-date audit of the data they collect on their clients and customers, keeping only what is essential to operations. This information must be **encrypted and secured.**

In-house or external resources in case of a data breach should include a **technical forensics analyst, legal counsel and communications specialist** to enable an immediate response and damage limitation.

Gallagher

Insurance | Risk Management | Consulting

Have the right cover

A comprehensive **cyber insurance program** needs to cover multiple risks, from financial loss to legal costs, and should be put together by a broker who understands both your operation and how a data breach could impact it.

Gallagher's team of cyber insurance specialists has the knowledge, capacity and ability to identify and protect an organisation's risk exposures.

Call **1800 240 432** or visit **info.ajg.com.au/contact-us** for obligation free advice.