Mandatory Breach Notification is Here

At midnight on Thursday 22nd February 2018 Australia's new requirement to mandatorily report on data breaches came in to effect. This means that if your organisation is "aware of reasonable grounds to believe an eligible data breach has occurred" you are obligated to inform individuals at risk of serious harm and to also notify the Office of the Australian Information Commissioner.

As your organisation considers the potential impacts of this new requirement, IPSec can provide you with guidance and assistance in all aspects of compliance with the new mandatory breach notification requirements.

What sort of breach do you need to notify about?

The mandatory breach notification requirements state that a "notifiable breach" is anything that causes disclosure of information that could cause serious harm. A notifiable breach is deemed to occur if the following three criteria are met:

1. An unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information has occurred;

2. The disclosed or lost personal information is likely to result in serious harm to one or more individuals; and

3. Your organisation has not been able to prevent the likely risk of serious harm with remedial action.

What should be done to prevent or manage a notifiable breach?

IPSec, based on the advice of the Office of the Australian Information Commissioner, advises that the following should be undertaken and/or in place to help identify, respond to, mitigate, and/or remediate breaches:

- **Governance, culture, and training**

  Organisations should adopt a culture of protecting personal information (of clients, employees, suppliers, and partners). This should be reflected in regular staff training, policies and procedures, and general organisation governance practices.

- **Internal practices, procedures, and systems**

  The Australian Privacy Principles requires that organisations take reasonable steps to enact and maintain practices, procedures, and systems to ensure compliance with the privacy principles.

- **ICT security**

  Your organisation should have in place effective controls and practices to protect both the hardware and software from misuse, interference, loss, unauthorised access, modification, and/or disclosure.

  Organisation's need to consider the cyber security of all of their systems. This includes websites, social media platforms, mobile device applications, mobile devices, portable storage devices, desktop workstations, kiosks, wired and wireless networks, remote access mechanisms, data storage systems, data processing systems, and all other aspects of your information environment that may contain, use, or provide access to personal information.

  Your organisation should ensure that the security mechanisms that are adopted and maintained appropriately through the use of regular security testing regimes such as penetration testing, security solution reviews, and security practice gap assessments.

- **Access security**

  Organisation's should have in place security controls and practices to not only prevent and identify external threats but to also address threats from trusted insiders (whether as an act of malice or accidental breach).

  It is important that organisations establish and maintain adequate identity management and authentication mechanisms and ensure that non-public information is not held on publicly accessible systems.

  Organisations must also ensure that they have adequate audit logging, audit trails, and monitoring to permit the rapid identification and classification of breaches. It is very important that all organisation have a central repository of audit log data that is capable of rapidly identifying when a breach occurs and that expedites the time required to investigate breaches and their impact.

- **Third party providers (including cloud computing)**

  If your organisation outsources part or all of their personal information handling you will need to consider whether the third party provider is able to fulfil your personal information protection obligations on your behalf.

  Have you conducted appropriate due-diligence, have you considered the scope of information held by the third party, have you considered what controls the third party has in place to prevent a breach, and have you included specific terms in your contracts to deal with personal information security obligations?

- **Data breaches**

  When a data breach occurs it is important that your organisation has a response plan and that it includes clear lines of authority, communication, and responsibility that can assist you to rapidly contain the breach and manage your response.

- **Physical security**

  Security personal information requires adequate physical security to also be in place. This not only include the physical access to ICT systems and the information environment but also to physical (e.g. printed) copies of personal information and whether the workspace itself is conducive to secure practices.

- **Destruction or de-identification of personal information**

  If you organisation holds personal information that it no longer needs it is a requirement of the Australian Privacy Principles that the organisation takes reasonable steps to destroy or de-identify the information.

- **Standards**

  IPSec recommends that organisations consider the adoption of an appropriate information security standard to provide an industry based point of reference for its personal information security objectives.

For more information on actions to be prepared for the requirements of mandatory breach notification IPSec recommends review the following document from the Office of the Australian Information Commissioner.

https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information#part-b-steps-and-strategies-which-may-be-reasonable-to-take

What happens when a breach occurs?

The unfortunate reality for all organisations is that breaches are not 100% preventable. Whilst it should be the objective of every organisation to put in place preventative mechanisms to stop breaches and to limit the impact of breaches that do occur, it is necessary to have in place the mechanisms to respond to a breach when they happen.

When the organisation has reasonable grounds to believe that a notifiable breach has occurred they are obligated (from 22nd February 2018) to notify individuals at likely risk of serious harm, and to notify the Office of the Australian Information Commissioner.

In fulfilling the organisation's notification requirements they must prepare a statement and provide a copy to the OAIC. The statement must include the name and contact details of the entity, a description of the data breach, the kind(s) of information involved, and what steps are recommended for impacted individuals to take to reduce their risk.

If it is not practical for the breached organisation to notify individuals they are required to publish a copy of the statement on the organisation's website and take reasonable steps to publicise the contents of the statement.

For further reading on this, IPSec recommends you review the following document from the Office of the Australian Information Commissioner.

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

APAC CIO Outlook TOP 25
CYBER SECURITY
TECHNOLOGY COMPANIES - 2017

APAC CIO Outlook 10 Most Promising
RISK MANAGEMENT
SOLUTION PROVIDERS - 2017

For more information or if you'd like a demonstration of IPSec vSOC's capabilities please contact your IPSec account manager.

1300 890 902

enquiry@ipsec.com.au

ipsec