September 2020

Corporate & Commercial Insights

Key insights from July 2020 OAIC Notifiable Data Breaches Report

The Notifiable Data Breaches (**NDB**) scheme was introduced in February 2018 to improve consumer protection and security relating to personal information. The Office of the Australian Information Commissioner (**OAIC**) recently released its half-yearly Notifiable Data Breaches Report (**NDBR**) for the period from 1 January to 30 July 2020. The NDBR provides detail around the causes and sources of data breaches reported under the NDB scheme, and highlights emerging issues relating to the protection and potential misuse of personal information. Notifications made under the *My Health Records Act 2012* are not included in the NDBR as they are subject to specific notification requirements set out in that Act.

Under the NDB scheme, a data breach is considered an 'eligible data breach' where the following three criteria are satisfied:

- there is unauthorised access to or unauthorised disclosure of personal information (or loss of personal information that an entity holds);
- a reasonable person would conclude that the access or disclosure is likely to result in serious harm to any of the individuals to whom the personal information relates; and
- the entity has not been able to prevent the likelihood of serious harm by taking remedial action.

Key findings in the NDBR include

- 518 breaches were notified under the NBD scheme in January to June 2020. This figure represents a 3% decrease from the 532 data breaches notified in the previous six month period (July to December 2019), but up 16% on the 447 notifications received during the like period January to June 2019.
- Malicious or criminal attacks (including cyber incidents) remain the leading cause of data breaches, accounting for 317 (or 61%) of all notifications.

- Data breaches resulting from human error account for 34% of all breaches.
- The health sector is the highest reporting sector, notifying 22% of all breaches. Human error is the leading source of data breaches reported in the health sector.
- After health, finance (including superannuation) is the second highest reporting sector, notifying 14% of all breaches, followed by education (8%), insurance (7%), and legal, accounting and management services (5%). Malicious or criminal attacks are the leading source of data breaches in the finance sector.
- Most data breaches affected less than 100 individuals. This is consistent with trends from previous reporting periods.
- Contact information (such as an individual's home address, phone number or email address) remains the most common type of personal information involved in a data breach.

Cyber incidents (specifically incidents of phishing, malware, ransomware, brute-force attack and compromised or stolen credentials) were the largest type of malicious and criminal attacks reported during the period January to June 2020, accounting for 218 notifications. From January to June 2020, the number of data breach notifications attributed to ransomware attacks increased by more than 150% compared to the previous six month period- increasing from 13 to 33. Ransomware is a kind of software which can be installed through email attachments or webpages, which encrypts the data stored on the affected system, rendering the data either unusable or inaccessible. The malicious actor behind the attack often exploits vulnerabilities in a system for financial or other gain.

Data breaches are a potential risk for businesses, not just in monetary terms, but also in terms of loss of confidence, reputation and trust from clients and customers. This is particularly topical due to the increased reliance on technology as a result of the COVID-19 pandemic. The average costs of a data breach involving malicious or criminal attack for a business has been reported to be $276,323[1] per incident. The NDBR is a timely reminder for businesses to ensure they have all necessary precautions in place to prevent otherwise avoidable data breaches. This includes consistently reviewing and improving internal security systems used to protect personal information from theft and misuse (including cyber-attacks), and considering whether the entity has adequate cyber protection in place should a cyber-attack occur.

[1] https://www.communications.gov.au/sites/default/files/Cost%20of%20cybercrime_INFOGRAPHIC_WEB_published_08102015.pdf?acsf_files_redirect

Further Resources

The full July 2020 NDBR can be found at https://www.oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/Notifiable-Data-Breaches-Report-Jan-Jun-2020.pdf

The OAIC and the Australian Cyber Security Centre publish comprehensive advice on preventing data breaches. Details can be found at https://www.oaic.gov.au/privacy/notifiable-data-breaches/preventing-data- breaches-advice-from-the-australian-cyber-security-centre/. This includes tips for setting passwords and improving staff awareness.

Meridian Lawyers regularly advises clients on privacy and the appropriate strategies to have in place to minimise the potential for data breaches to occur. This article was written by Special Counsel, Hayley Bowman with the assistance of Graduate Lawyer, Molly Cooke. Please contact us if you have any questions or require further information.

Hayley Bowman
Special Counsel
+61 3 9810 6723
hbowman@meridianlawyers.com.au

Molly Cooke
Graduate Lawyer
+61 3 9002 2105
mcooke@meridianlawyers.com.au

Disclaimer: This information is current as of September 2020. This article does not constitute legal advice and does not give rise to any solicitor/client relationship between Meridian Lawyers and the reader. Professional legal advice should be sought before acting or relying upon the content of this article.