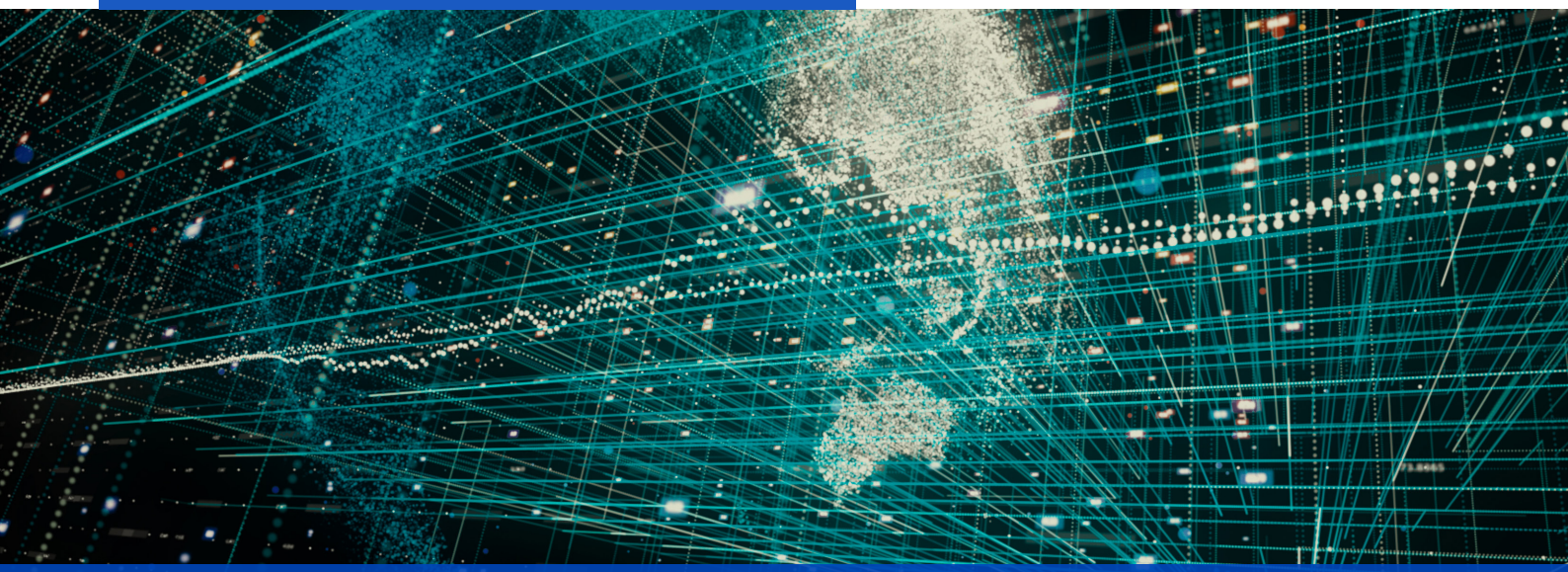
PRIVACY REPORT



BY ALBERT YUEN

AUGUST 2018

AUSTRALIA'S LATEST DATA BREACH REPORT REVEALS INCREASING NOTIFIABLE DATA BREACHES

Mandatory personal data breach notification laws were introduced in Australia in February 2018 which required organisations to notify data breaches likely to result in serious harm to any individuals to those persons and the Australian Information Commissioner (the Notifiable Data Breaches (**NDB**) scheme).

On 31 July 2018, the Office of the Australian Information Commissioner (**OAIC**) released its Notifiable Data Breaches Quarterly Statistics Report for the period 1 April to 30 June 2018 (the Report) relating to the NDB scheme.

The NDB Report July 2018 is the first full quarter of operation of the NDB scheme since it commenced on 22 February 2018, with the first OAIC NDB scheme quarterly statistics report (which covered the period 1 January to 31 March 2018) (First Report) covering only a part period given the NDB scheme took effect on 22 February 2018.

The aim of these OAIC NDB reports is to provide statistical information on data breaches occurring in Australia and the reasons why they happen in order to inform organisations to take steps to prevent reoccurrence.

KEY TAKEAWAYS

1. **The number of data breach notifications to OAIC and individuals are increasing.** 242 notifications were received in this Report, compared to 63 under the First Report. Notwithstanding the lack of 'like for like' for the length of reporting periods between this Report and First Report, the telling statistic is there has been month-on-month increases in the number of data breaches each month during the NDB scheme. OAIC indicates that the increasing number of notifications under the NDB scheme demonstrates awareness by entities of their obligations to notify the OAIC.

2. **The top five industry sectors reporting data breaches are (1) health, (2) finance, (3) legal, accounting and management services, (4) education and (5) business and professional associations.** The health and finance sectors comprise over a third of the total number of reported data breaches under the NDB scheme for the quarter, even though notifications made under the My Health Records Act 2012 are not included in report (as they are subject to specific notification requirements set out in that Privacy Act).The health sector represented the top sector reporting data breaches under the First Report, with the finance sector coming in third.

3. **The main causes of data breaches are malicious or criminal attacks (142 notifications or 59 per cent), followed by human error (88 notifications or 36 per cent).** Malicious or criminal attacks included phishing, malware, ransomware, brute-force attacks, compromised or stolen credentials or other forms of hacking, but also included theft of paperwork and storage devices, for example USBs.

4. **Many cyber incidents appear to have exploited vulnerabilities in organisations involving a human factor.** Human factors/ errors contributed materially to data breaches, such as personnel clicking on a phishing email or disclosing passwords). The most common human error was sending emails containing personal information to the wrong recipient. It is important to note that while technical cyber security capabilities and systems security is important, risks of data breaches can be greatly reduced by ensuring that staff responsible for handling personal information receive regular training to mitigate against human error.

The Report provides a timely reminder of the prevalence of data breaches in Australian businesses, the need to understand the key risks and take steps to protect personal information and to be prepared to assess and report data breaches to OAIC and individuals under the NDB scheme. Strong data management is integral to the operation of businesses and government everywhere, and the increasing use of digital platforms and technologies to connect with users and provide personalised products or services have increased the risks for data breaches.

For further information about the NDB scheme, assistance identifying and mapping out the applicable regulatory requirements for information held by your organisation privacy impact assessments or assistance in preparing a personal data response plan, please contact the author.

ALBERT YUEN
Special Counsel
T +61 3 8656 3316
E ayuen@gtlaw.com.au

SYDNEY
Level 35 International Towers Sydney
200 Barangaroo Avenue
Barangaroo NSW 2000
Australia
T +61 2 9263 4000
F +61 2 9263 4111

MELBOURNE
Level 22
101 Collins Street
Melbourne VIC 3000
Australia
T +61 3 8656 3300
F +61 3 8656 3400

PERTH
Level 16 Brookfield Place Tower 2
123 St Georges Terrace
Perth WA 6000
Australia
T +61 8 9413 8400
F +61 8 9413 8444