THE
NATIONAL LAW REVIEW

Q4 Notifiable Breaches Continue to Rise

Monday, February 18, 2019

The Office of the Australian Information Commissioner (OAIC) has released its fourth quarter report of notifiable data breaches between October – December 2018.

The report exposed that the OAIC received 262 notifications of data breaches, which has increased from the 245 notifications that were reported the previous quarter. Below are the key findings from their report:

Article By Rob PulhamK&L Gates
Cameron AbbottCyberwatch: Australia

Communications, Media & Internet
Global
Australia

- The OAIC report identified the top five sectors who reported data breaches. Private health service providers reported 54 breaches, the finance sector reported 40 breaches, professional services reported 23 breaches, private education providers reported 21 breaches and the mining and manufacturing industry has made its first appearance with a reported 12 breaches.
- 85% of data breaches involved individual's contact details, 47% involved financial details, 36% involved identity details, 27% involved health details, 18% involved tax file numbers, and 9% involved other types of personal information.
- The sources of breach varied, with 64% of data breaches due to malicious or criminal attack, 33% due to human error, and 3% due to system faults.
- The report also breaks down the breach types per industry. Interestingly, the finance sector experienced the most malicious cyber attacks, and human error dominated the healthcare sector.

Even though 60% of the total breaches involved personal information of 100 individuals or fewer, there were a couple of notifications affecting a significantly higher number of individuals (including one that affected more than 1 million individuals). Human error breaches resulting in the unauthorised disclosure of personal information (via unintended release or publication) impacted an average of more than 17,000 individuals per breach (though this average seems likely to have been skewed by some particularly large breaches), and the failure to securely dispose of personal information affected an average of 300 individuals per breach.

Most data breaches resulted from malicious attacks which gain access through compromised credentials (such as phishing emails or stolen username and passwords). So, if you believe that the email from your CEO requesting your bank details for your exorbitant raise is legitimate, think again!

Ella Richards contributed to this post.