Article Information

Authors: Andrea Beatty, Chelsea Payne
Service: Banking & Finance, Cyber Security, Privacy
Sector: Financial Services

OAIC releases its 12-month Notifiable Data Breaches report

The OAIC have released their first annual notifiable data breaches report, following the introduction of mandatory data breach reporting in February 2018.

The Office of the Australian Information Commissioner (**OAIC**) has released its 12-month notifiable data breaches report for the period 1 April 2018 to 31 March 2019.

During the period, of the 1,132 notifications made to the OIAC, a total of 964 eligible data breaches were reported.[1] This was a 712% increase in notifications since the scheme was made mandatory in February 2018.[2] Of the breaches reported, 86% involved the disclosure of contact information.[3]

60% of reported data breaches were as a result of malicious or criminal attacks, with phishing and spear phishing the most common and effective measure of attack.[4]

35% of attacks were attributed to human error, such as through unintended disclosure of personal information or the loss of a data storage device. However, this number rose to 55% for health sector data breaches and 41% for finance sector data breaches.[5]

83% of the reported breaches affected less than 1,000 people. 3 of the breaches affected over one million people however, 232 breached had only affected one individual. As has been seen in previous data breach cases, a data breach does not need to affect hundreds of people to be a serious breach. In August 2019, Ryde Hospital staff mistakenly handed the medical records of a sexual assault victim to another patient, which contained personal contact details and private medical information regarding the sexual assault. In 2011, medical company MedVet revealed the names, home and work addresses of 692 MedVet customers who had ordered paternity, drug and alcohol test kits were made available on the internet.

The OAIC notes that consumers benefit most from timely notifications in plain English that explain the key risks and how they can mitigate them.

[1] Office of the Australian Information Commissioner, 'Notifiable Data Breaches Scheme 12-month Insights Report' (13 May 2019).
[2] Ibid.
[3] Ibid.
[4] Ibid.
[5] Ibid.