Victoria Geddes
Executive director
FIRST Advisers

MANDATORY DATA BREACH REPORTING KICKS OFF

Early reports indicate notifications to the regulator are on the rise.

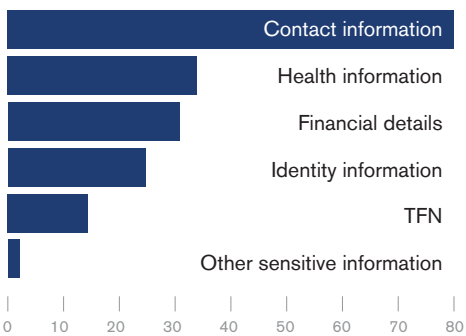
Data from the first five weeks of the federal government's new scheme for the mandatory reporting of cyber security breaches was released on 11 April 2018. Every private and public company with annual turnover of $3 million or more, listed or not, is now required to report a cyber breach to the Office of the Australian Information Commissioner (OAIC) and notify affected customers as soon as it becomes aware of a breach. Any breach that is likely to result in serious harm to an individual is reportable. This could occur when there is unauthorised access to, disclosure or loss of customer information held by an entity. Such information includes personal details, credit reporting information, credit eligibility information, and tax file number information. Companies must report the breach within 72 hours.

The score card one month in

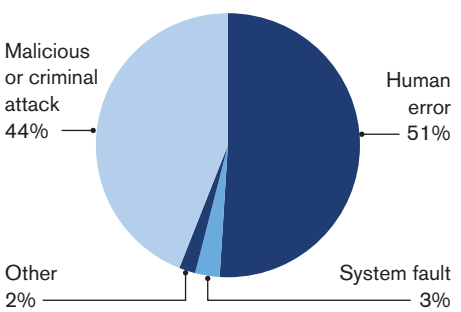
The OAIC had optimistically predicted the new mandatory requirements for notification would double the number of reported incidents each year. The initial data reveals there were 63 notifications in the first five weeks of the scheme compared to 114 notifications for the 2017 financial year under the previous voluntary scheme. The majority of data breaches to date have involved contact information (78 per cent), or an individual's name, email address, home address or phone number. This is distinct from 'identity' information (24 per cent) which refers to driver's licence and passport numbers. Health information and financial details such as bank account or credit card numbers were each represented in around a third of reported breaches.

Human error (51 per cent) and malicious or criminal attacks (44 per cent) accounted for almost all of the breaches. Just over half of the notifications involved the release of personal information of between one and nine individuals with 27 per cent of notifications involving more than 100 individuals. The scheme has yet to deal with a large-scale breach involving more than 100,000 people. That will be when the communication component of an organisation's cyber incident response plan, assuming it has one, is really put to the test.

Type of personal information breached



Source of breaches reported



Healthcare leads breaches

Five sectors accounted for 66 per cent of all reported breaches with health service providers leading the pack (23 per cent), which is comparable to the global picture in 2017 where the top five industry sectors accounted for 72 per cent of all breach incidents with healthcare accounting for 26 per cent.

Where Australia differs from the global experience is the level of breaches coming from professional services firms, which comprised 16 per cent of all incidents, compared to only five per cent globally. But these statistics are based on such a small sample it would be unwise to be definitive about drawing firm conclusions.

Preparedness to report

FIRST Advisers surveyed ASX 300 companies during September and October 2017, seeking feedback on their readiness for mandatory reporting of cyber security breaches in 2018. The responses were sharply divided according to company size and sector.

Small cap companies and those in the metals and mining sector had yet to establish frameworks for reporting on or addressing this risk. Large cap companies, particularly those in the financials and Australian real estate investment trust (AREIT) sectors, were much more confident they were properly prepared for a cyber incident. They were generally well organised (83 per cent), with comprehensive response plans in place that covered all main stakeholders. The less well-resourced small cap companies were struggling to meet this standard (23 per cent).

The survey gathered feedback on a range of issues including management awareness of and preparedness for the change in reporting protocols, how they communicated their risk profile to the investment community and whether they had a cyber incident response plan and crisis management plan in place that was periodically updated and tested.

The results were summarised in the report *Listed Company Readiness for Mandatory Reporting*, which can be downloaded from www.firstadvisers.com.au