Article Information

Author: Tim Clark
Service: Cyber Security, Intellectual Property & Technology, Privacy & Data Protection
Sector: IT & Telecommunications

Update on Australia's Notifiable Data Breaches scheme

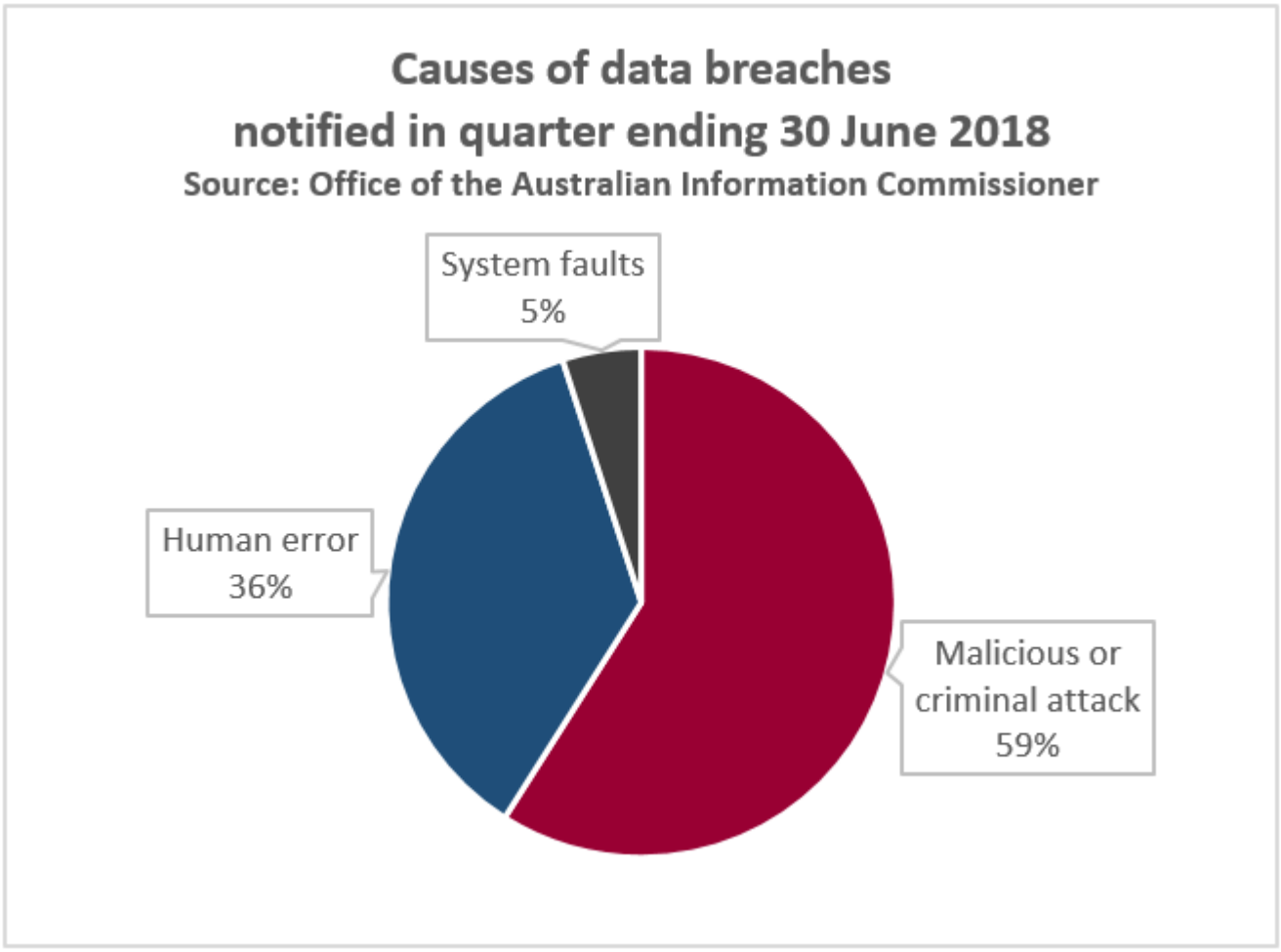
In our earlier article 'Data Breach Response Planning: Getting Down to Business' we referred to the introduction of a mandatory new Notifiable Data Breaches (NDB) scheme in Australia and outlined some steps organisations could take to prepare. The changes were introduced by the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth).

The new law requires entities covered by the *Privacy Act* 1988 (Cth) to notify both the Office of the Australian Information Commissioner (**OAIC**) and affected individuals of any data breach in respect of personal information they hold where the breach is likely to result in serious harm.

We are now seeing how the mandatory NDB scheme is operating in practice. The OAIC has just released its second quarterly statistical report on notifications under the NDB scheme (**NDB Report**). You can access their news release and a link to the Report here.

Overview

The NDB Report indicates that a total of 242 notifications were received in the quarter ending 30 June 2018. Although this is the OAIC's second such report, the previous report only covered a period of a few weeks (and reported 63 notifications). So, this NDB Report represents the first full quarter of data since the NDB scheme commenced on 22 February 2018.

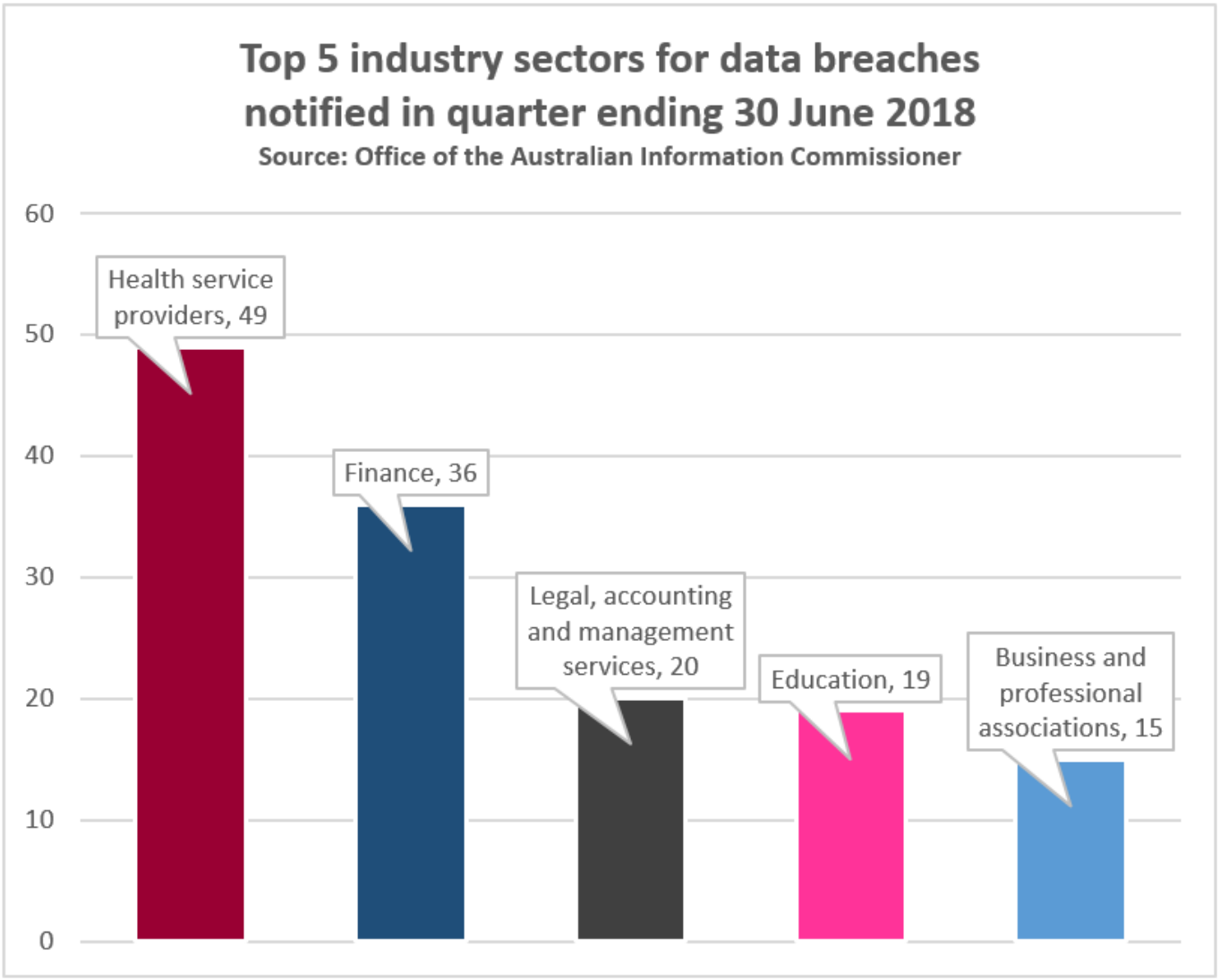


The single largest cause of data breaches that were reported in the quarter was malicious or criminal attack (59%), followed by human error (36%). The cause of the remaining 5% of data breaches was notified to be system faults.

Malicious or criminal attack

Malicious or criminal attacks are those deliberately crafted to exploit known vulnerabilities for financial or other gain. The single largest type of malicious or criminal attack were described as “cyber incidents”. These include phishing, malware, ransomware, brute-force attack, compromised or stolen credentials (e.g. user ID and password) and hacking by other means. It includes social engineering attacks (where an outside attacker manipulates personnel inside the organisation usually to avoid standard security protocols) or impersonation or actions taken by a rogue insider.

One of the most common forms of cyber attacks is phishing. **Phishing** involves an attempt by an attacker to trick a person into disclosing personal information such as bank accounts, login IDs, passwords or credit card numbers by pretending to be contacting them from a legitimate source. It is a relatively common form of cyber attack and can lead to significant financial fraud: see the Australian Competition and Consumer Commission’s Scamwatch report for more details. It is no surprise that the data reveals a large number of phishing attacks: humans are often a weak link in an organisation’s security systems. However, this should not necessarily be seen as a criticism of staff in general. Phishing attacks are becoming increasingly sophisticated, with attackers often undertaking research on target organisations leading to more apparently genuine correspondence, often targeting specific individuals or roles within organisations.



Whilst cyber incidents are the most common, there are some "old school" forms of malicious attacks. **Theft of paperwork or storage devices** was also a significant source of malicious or criminal attacks. This serves as a timely reminder that information security is not just about technology and telecommunications infrastructure and networks, but also includes the control and security of paper and other physical records, controls on use of removable media such as USB sticks and a need to take care of portable computing devices such as laptops (such as by not leaving them unattended in locations where they could easily be stolen).

Since the introduction of the NDB scheme, Piper Alderman has advised clients in relation to notifications under the NDB scheme involving phishing as well as theft of paperwork or storage devices. Where required, we have prepared for clients draft notifications to the OAIC and affected individuals.

Health sector is the top sector affected overall

The top sector overall in terms of data breaches notified was health service providers (49 notifications or 20% of the total notifications). However, the NDB Report makes clear that this number only includes **private** sector health entities. State or Territory public hospitals and health services are bound by State and Territory privacy laws and are not included in the NDB Report. There is also a separate notification scheme under the *My Health Records Act* 2012 (Cth). So, the true picture on health sector data breaches is likely to be even more concerning .

Healthcare providers often hold or process large volumes of personal information, including sensitive health information as well as financial information such as credit card data. Whilst malicious or criminal attacks were involved in a number of notifications in the health sector, more than half of data breach incidents in the health sector (29 breaches) were stated to be due to human error. This generally involved sending personal information to the wrong recipient via email or post.

Other 'top 5' sectors

Other significantly affected sectors were the finance sector with 36 notifications (15%), legal accounting and management

services with 20 notifications (8%), education with 19 notifications (8)% and business and professional associations with 15 notifications (6%). Together, the top 5 sectors account for 139 notifications of data breaches or 57% of the total notifications.

What types of personal information were compromised?

The single largest category of personal information affected by notified data breaches was contact information (89% of notified breaches). Other types of personal information included financial details (42%), identity information (39%), health information (25%) and tax file numbers (19%). Whilst unauthorised access to contact information may often be perceived by organisations as being a relatively lesser risk, access to contact information of individuals can often be used in subsequent phishing attacks on that individual, sometimes involving attackers having combined that information with publicly available information about the individual (such as on social media). The relatively high number of data breaches involving tax file numbers is concerning particularly given that the Australian Privacy Principles and other privacy regulations specifically regulate the use of tax file numbers of individuals as being particularly sensitive.

Conclusion and next steps

As the OAIC has noted in its NDB Report, understanding the main causes of data breaches should help everyone to take steps to prevent occurrence (or recurrence). It is best to prepare now to minimise the likelihood of a data breach in your organisation as well as to have a well-considered plan as to how to deal with a data breach if it does occur.

All businesses need to ensure that appropriate IT governance and security policies are in place to clarify and define the organisation's security systems, policies and procedures. It is also crucial that training and awareness campaigns are conducted regularly within an organisation (particularly around the more common forms of attacks such as phishing) so that employees know what to look out for and what to do.

Piper Alderman regularly advises clients, and conducts workshops and training, on the NDB scheme (and privacy laws more generally), data breach notification policies and plans and requirements for notification under the NDB scheme. Where data breaches have occurred and are likely to cause significant financial or other harm, it is also important for organisations to engage with their lawyers as early as possible to assist in maintaining client professional privilege in relation to internal and external investigations of the data breach.