Cyber attack revelation highlights need to prepare for mandatory data breach reporting

Data breaches have been running hot in the news lately following the revelation of a successful cyber attack on a national security contractor.

This particular breach occurred in July 2016 and involved hackers gaining access to the computer system of the contractor and stealing sensitive information about Australia's warplanes and navy ships. Authorities were only alerted to the breach in November 2016.

Data breaches are a concern to any business – large or small – that holds sensitive information. However, keeping quiet about breaches that could result in harm to an individual will no longer be possible with the new mandatory breach notification scheme coming into effect from next year.

From February 28, 2018, if a business experiences a data breach and believes that serious harm may result to any individual affected by it, then that business needs to notify the Privacy Commissioner and the affected individuals.

This follows the passing of the *Privacy Amendment (Notifiable Data Breaches) Act 2017,* which introduces mandatory data breach notification obligations for all organisations subject to the Act (Cth). This includes all Australian-registered companies.

The move brings Australia in line with other countries – mandatory disclosure was introduced 15 years ago in the United States – and also provides consumers with greater clarity about the privacy of their personal information.

Data breaches are defined as those in which there is unauthorised access, disclosure or loss of personal information held by an entity, which is likely to result in serious harm to any of the individuals to whom the information relates.

So what is serious harm? It can include physical, psychological, emotional, economic and financial harm, as well as harm to reputation. The "serious harm" test is assessed on a case-by-

case basis, which means that the harm doesn't need to have been suffered by all individuals affected by the breach.

Once they believe a data breach has occurred, businesses need to carry out a "reasonable and expeditious" assessment and notify any individual affected as well as the Privacy Commissioner. They need to take reasonable steps to complete the assessment within 30 days after becoming aware of the breach.

Information provided should include the company's name, a description of the breach, the kind of information concerned, and recommendations around what steps the individual could take to deal with the breach.

Key steps

Andrew Spring

Jirsch Sutherland Partner Andrew Spring says businesses should be taking action now to ensure they have a data security strategy in place.

"Brand and reputational damage are common consequences of a data breach, and this could have disastrous financial implications for a business," he says. "Action should be taken now to limit the possibility of a breach occurring. This includes updating software, defining what a breach is and nominating someone to be responsible for identifying and dealing with any breaches."

Other actions a company can take to prepare for the new mandatory reporting regime include:

- Produce a policy and procedures document that defines "serious harm" and what action needs to be taken in the event it occurs.
- Review contracts with suppliers and service providers to ensure they have implemented data security measures.
- Have a draft notification in place so it is ready to send in the event action needs to be taken.

Remember if you fail to inform those affected by a data breach, you may be fined under the

Privacy Act. Penalties of up to $1.8 million for companies and $360,000 for individuals may be imposed for serious or repeated breaches.