MANDATORY DATA BREACH REPORTING: HOW IT AFFECTS YOU!

AUTHOR // PETER KARCHER

MARCH 2017

WHOOPS, YOUR HEAD OF SALES JUST LEFT THE COMPANY LAPTOP ON THE BUS. TIME TO INFORM THE PRIVACY COMMISSIONER?

Lost laptops and portable devices containing personal information are among the examples listed by the Office of the Australian Information Commissioner in its guide on data breaches. It will soon be mandatory under Australian law to report certain data breaches, and inform affected individuals, where personal information has been the subject of unauthorised access or disclosure.

The term "data breach" brings to mind first and foremost a cyber attack by nameless ghosts out there in the Internet, an extraordinary circumstance affecting high profile businesses or big corporates. In fact the Explanatory Memorandum to the recent changes in the law cites a 2014 Australian report which found nearly a quarter of businesses surveyed had suffered an IT security breach in the previous 12 months, and 60% had suffered a breach in the previous five years. A PwC report found 38% more security incidents were detected in 2015 than in 2014.

A far more common data breach, for example, is the email which inadvertently goes out to your customer database while displaying the email addresses of all the recipients! Or the employee who mistakenly discloses customer information to the wrong person at another organisation, when the employee was not actually authorised to disclose it, or the recipient may not have been authorised to receive it!

WHEN DO YOU NEED TO REPORT?

But when do you need to report such a breach, and, more importantly, contact the individuals whose information is at risk? The answer is: only when there is a "likely risk of serious harm" to any of the affected individuals. Understanding what that means is going to pose a big challenge to many businesses. "Likely" means "more probable than not". That's fairly straightforward, but it's the "serious harm" component which gets a bit more tricky.

The law doesn't set out all the circumstances in which "serious harm" may occur. While the Explanatory Memorandum acknowledges that "financial, economic or physical harm" are more likely to be "serious", it points out that psychological or emotional harm, or harm to reputation, may be serious harm for the purpose of the compulsory notification. So while the disclosure of customers' credit card details, for example, has the clear potential for serious harm, will the disclosure of a database of names, email addresses, phone numbers etc be a notifiable breach?

The unsatisfactory answer is: it depends. For example, names and addresses of individuals may not ordinarily be sensitive information. But if that information relates to individuals who are accessing a particular government service, or who are clientele of a particular business, sensitivity may nonetheless arise if the knowledge that the individual was accessing the service or was a client of the business could cause harm.

WHO DOES THIS AFFECT AND WHAT DO I NEED TO DO NOW?

The good news for small business is that the new law will only affect those businesses already subject to the *Privacy Act*, that is, businesses with annual turnover in excess of $3 million, or businesses with a lesser turnover who deal in personal information.

But for the many medium and large sized businesses that the mandatory notification affects, advance preparation is going to be key. Businesses will need to look at a range of increased security measures such as encryption technology, to minimise the risk of "serious harm" if there is a data breach. The new law also provides an exception where certain remedial action is taken quickly on discovering a data breach, including in the case of a "loss" of data, taking steps to ensure that the lost data cannot be accessed or used. Remote wiping of information from portable devices is one preventative measure which could be useful in those circumstances.

But businesses will need to turn their mind to these matters in advance. Waiting until a breach occurs is a recipe for disaster, especially given the particulars which need to be notified to affected individuals if a breach occurs. These include recommendations about the steps that individuals should take in response to the serious data breach. Businesses will therefore be forced to turn their minds to the possible range of breach scenarios and how to deal with them. That is something that will be difficult to do on the fly once a breach occurs.

Actual penalties are unlikely to be anywhere near the potential maximums of $360,000 for individuals and $1.8 million for organisations, except in exceptional or flagrant circumstances. However the cost of dealing with a reportable data breach, in terms of hard dollars, as well as damage to reputation, means businesses will want to get well out ahead of these laws and avoid the breach in the first instance.

PETER KARCHER IS HEAD OF THE CORPORATE & COMMERCIAL PRACTICE GROUP AT CLARKEKANN LAWYERS. HE IS A COMMERCIAL LAWYER WITH PARTICULAR EXPERTISE IN INTELLECTUAL PROPERTY, TECHNOLOGY AND DATA PROTECTION LAW.

FOR MORE INFORMATION, PLEASE CONTACT:

PETER KARCHER //
Partner

T 61 2 8235 1218

E p.karcher@clarkekann.com.au