



# Honey, there's something I should tell you...

AS AUSTRALIA WEIGHS THE OPTION OF FOLLOWING THE UNITED STATES AND EUROPE IN GUARDING AGAINST DATA SECURITY BREACHES, ACXIAM'S

JODIE SANGSTER EXAMINES THE PROS AND CONS OF INTRODUCING MANDATORY NOTIFICATION LEGISLATION.

**D**ata is considered by some to be the single most valuable asset of any customer-driven organisation. Despite this increasingly widespread view of data's significance to the business, it is not often treated with the same degree of value or respect as other, more tangible company assets. Nor is it, in many instances, protected to the same degree as its more material counterparts.

The existing distinction between tangible and non-tangible business assets may soon become a thing of the past. The Government plans to introduce data security breach notification laws will soon

Tax Office followed up the incident by sending security breach notification letters to all affected, accidentally disclosing yet more personal data. This breach was considered so serious that it led to calls for the resignation of the UK Chancellor of the Exchequer, Alistair Darling, and even the Prime Minister.

Similar breaches have occurred all over the world. In the USA, retailer TJ's fell victim to hackers who infiltrated its customer database and obtained the credit card details of almost 95 million customers. Similarly, in Europe, Scandinavian bank, Nordea, found itself subjected to a prolonged attack. Over the course of fifteen months the bank was targeted by emails containing tailor-made software, which allowed hackers to take over its online bank accounts. As a result, more than 250 customers were subjected to fraud.

## Getting it out into the open

No doubt countless other major security breaches have occurred in Australia and throughout the world. The majority of these would have been handled internally and dealt with quietly, with consumers and regulators none-the-wiser that such incidents had ever come to pass.

No longer. The Rudd Government is considering a proposal put forward by the Australian Law Reform Commission (ALRC), recommending the introduction of mandatory data security breach notification laws in Australia. This would require any Australian organisation responsible for a data security breach to inform both the Office of the Federal Privacy Commissioner (OFPC) and any affected consumers of what has occurred. Once reported, nothing would prevent the incident from being publicised, or stop further OFPC investigation. Should the organisation be found in breach of the Privacy Act, appropriate penalties would then be imposed.

Though this should be regarded as fair punishment, it seems to provide little incentive for businesses to admit wrongdoing. The USA has had State-based

legislation for many years, placing obligations on companies that are responsible for data security breaches. These laws require active notification of individuals by US organisations if a security breach has occurred, or may potentially have occurred. Europe has followed suit, with countries such as Germany, Spain, Hungary, Malta and Sweden introducing some breach notification requirements.

## Time to 'fess up

Feedback on data security breach notification laws has been mixed. Though such data legislation has been viewed positively for the most part, increasing concern over the compliance burden placed on business and the potential 'cry wolf' consequences of consumers becoming inundated with data breach notices has arisen.

To avoid similar issues in Australia, the ALRC recommended the establishment of a threshold; organisations would be required to notify of a breach where personal data has been, or is reasonably believed to have been, acquired by an unauthorised person, and that unauthorised acquisition may give rise to a real risk of serious harm to any affected individual.

Although it may be a number of months before the introduction of mandatory breach notification legislation in Australia, the OFPC is planning to introduce a voluntary breach notification scheme. This will blaze a trail for the establishment of a mandatory scheme in the future, enabling organisations to gradually become accustomed to the idea of data security breach notification laws.

Overall, the message is loud and clear: protect your data or suffer the consequences. 📍



**The message is loud and clear: protect your data or suffer the consequences.**

make organisations both responsible and accountable for the protection of the data they hold. In addition, companies negligent in the area of data security will be required to publicise their shortcomings and inform their customers of their mistakes—a potentially catastrophic reprimand for businesses reliant on strong brand and consumer trust.

## Something must be done

Data security breaches are on the rise, with five of the ten largest incidents in history occurring within the past year. The largest to date happened in November 2007, when headlines in the United Kingdom and around the world announced the admission by a UK government department of the loss of two disks containing the names, addresses, birth dates and National Insurance numbers of over 25 million people—that's almost half the adult population of the United Kingdom. Worse was to come, when the

Jodie Sangster is the Chief Privacy and Compliance Officer of Acxiom Australia and New Zealand.  
<jodie.sangster@acxiom.com>