Mandatory Data Breach Notification

Author: Aarron Spinley – Sense of Security Pty Ltd
Southern Region Business Manager
Issue Date: 21 May 2013

Amendment to the Privacy Act

In Early May, the Exposure Draft Privacy Amendment (Privacy Alerts) Bill 2013 was circulated to a small group of "stakeholders", which confirmed what many have long expected; that the Government plans to introduce mandatory data breach notification to Australia.

Background – This will happen

After an initial recommendation by the Law Reform Commission in 2008, the Federal Attorney General's Department has been considering submissions since late 2012 on the suitability of data breach notification (DBN) in Australia.

Notably, the Privacy commissioners of all states agree that DBN rules are necessary and may instigate their own local legislation, whilst at a Commonwealth level the Attorney General Mark Dreyfus has strongly indicated his support of the legislation.

It is reasonable then to conclude that the amendments will pass. In fact, some media have reported that it come into effect as early as July this year, if not early 2014. Perhaps tellingly, the Privacy office has released a revised guide to the possible DBN rules which urges organisations to prepare in advance.

So what are the potential consequences to an Organisation?

It has been widely reported in the media that the legislation will require organisations affected by a data breach (lost or stolen) to notify the Federal Privacy Commissioner, as well as the affected individuals, and in some instances the media. Specifically:

- Impacted organisations will have to provide a full and prompt disclosure statement to the Privacy Commissioner, including information such as the details of the event, the specific compromised data, and the remedial steps that affected parties should take.
- The affected individuals must also be separately notified.
- The Commissioner will have the powers to force the organisation to make a public statement on its website and to inform media outlets.

Subsequently, purely from a reputational risk standpoint, this has the potential to be a game changer for many organisations.

In addition, first time and "small-scale" offenders may be fined up to $34,000 for individuals, and $170,000 for organisations; whilst repeat and serious offenders face penalties of up to $340,000 for individuals and/or $1.7 million for organisations.

So the risk is real.

How will it be applied?

However there are a number of tests that a breach will have to meet before it is required to be disclosed, some of which are subjective.

For example, only data breaches that are classified as “serious” must be reported. Of course, this term will be interpreted in various forms; as evidenced by moves to harmonise the law across Europe[1] and the same debate occurring in the US[2].

Here in Australia, the draft legislation attempts to clarify this to some extent, citing that the Federal Government would consider a data breach to be serious if an organisation is “delinquent in its requirements” to take “reasonable” steps to secure personally identifiable information (PII).

It defines this further to state that the breached data will need to expose individuals to a "real risk of serious harm" – damage to reputation and/or adverse financial impact - as a result of unauthorised access or disclosure of PII.

Fortunately for many organisations, there will likely be a limited grace period for the first year or possibly 18 months, subject to the judgement of the Privacy Commissioner in each instance.

What does it mean in real terms?

Firstly, it is important to understand what constitutes PII. If the definitions supplied in Wikipedia can be relied upon, which are consistent with our experience in the field, organisations will need to consider the following:

Types of Personally Identifiable Information		
Digital identity	Full name	Email address
Date of birth	National identification number	IP address (in some cases)
Birthplace	Vehicle registration plate number	Driver's license number
Genetic information	Face, fingerprints, or handwriting	Credit card numbers
Country, state, or city of residence	Gender or race	Name of the school or workplace
Grades, salary, or job position	Criminal record	Other data linked to PII
Specifically nominated by the Federal Government in the Draft Bill • Credit reporting and credit eligibility data • Breaches to Tax File Numbers		

Australian Information Commissioner John McMillan has stated that the “quality and effectiveness of the response can rank in importance alongside the gravity of the data breach”.

So the presence of sound incident response practices will be very important to mitigate any sanctions to an organisation in the event of a breach.

But how does an organisation go about ensuring an appropriate (read: proportionate) level of due diligence and preventative activity in the first place?

Sensibly, the draft bill does not prescribe its own set of specific technology and practice requirements. Given that relevant standards and references already exist, clearly there is no benefit in burdening organisations and the business community at large with the costs of yet further bespoke compliance. And herein lies the rub.

Organisations already have duty to protect all manner of sensitive information, not just PII…

[1] The Law Patent Group: http://goo.gl/lv1ch

[2] “An American Quilt of Privacy Laws, Incomplete”, The New York Times, 30 Mar 13: http://goo.gl/Hj64T

Therefore pre-existing good practice relative to the particular organisation and the industry that it participates in is likely to prevail.
In this regard nothing has changed.

For instance, authorised deposit-taking institutions must have regard to PPG 234[3] , just as government entities are directed to the ISM[4], PSPF[5] or specific State based requirements; and health organisations to NESAF[6]. Similarly, organisations that store, process, or transmit credit card information are regulated by PCI DSS[7] and so on.

More broadly, organisations can develop an information security management system (ISMS) aligned to ISO/IEC 27000-series, or indeed to certify the management system under ISO 27001; in either event ensuring that the ISMS is applied to PII as contemplated by this legislation.

Of course it will be important to demonstrate actual assurance activities are conducted to ensure the presence and effect of control, but again – this is nothing new.

A note on Cloud Services

A significant inclusion of the legislation is for those organisations that use cloud services. It will be their responsibility to ensure that their provider does not breach privacy law.

The burden falls on the organisation, not its providers, and so the ability to demonstrate due diligence in the selection, contracting, and management of those relationships is important.

Readers may be interested in the whitepaper "Visibility & Control of your Cloud Service Provider":

http://www.senseofsecurity.com.au/research/it-security-articles

Close

So where does all this leave us? Well, commonly accepted and long held information security good practice will remain just that.

In short, if your organisation has developed a suitable, formal information security program, much of your risk under the amendments is mitigated by default. Of course, it is true that your assessment of certain risks may now change, and perhaps require greater – or simply different - controls.

What is clear is that if you have an existing information security management system, it is certainly timely to review this in context of these changes.

Of course, if you are yet to implement one, perhaps the time is right.

[3] Prudential Practices Guide 234 – Management of security risk in information and information technology

[4] Information Security Manual

[5] Protective Security Practices Framework

[6] National eHealth Security and Access Framework

[7] Payment Card Industry Data Security Standard