Adam Davenport

It's no secret that the Privacy Act has a long way to go

Compliance will only ramp up once the law starts to bite

Australia has lagged behind most developed countries in relation to data protection. The key legislation is the Privacy Act, administered by the Privacy Commissioner. Amendments to the act became law in March 2014, when the commissioner was given new powers, including the ability to start proceedings without receiving a complaint and the ability to impose fines of up to $1.7 million.

It is timely to look at how the changes have been received and what, if any, impact they have had on companies in Australia.

Prior to the amendments, the commissioner had little real power to compel compliance with the National Privacy Principles. The office adopted a consultative approach designed to encourage compliance. Without full investigative powers and a lack of penalties, this approach produced little substantial progress despite significant effort.

Business is about assessing risk. Companies must balance the cost of compliance against the risk and potential consequences of non-compliance. The application of this equation has seen compliance with the Privacy Act – and data protection generally – rank well down the priorities of most Australian companies.

Certainly, many well-managed firms have policies designed to protect their own data and that of their customers. Some of these policies and technologies overlap with the requirements of the Act. Few companies made these investments because of the laws.

But there are several other legal and regulatory regimes that do get focus and priority. Examples are PCI-DSS, APRA and ACCC. All are successful in getting the attention of Australian business and securing compliance to their regulations. (See box)

Companies rate the risk of audit or investigation by PCI-DSS, APRA and the ACCC as high. The consequences of non-compliance are severe and adverse publicity can create damage to reputation and share value. These regimes get more priority than the Privacy Act has done. What they have in common is a culture of education, audit and strong enforcement.

So what have companies done in response to the new privacy laws?

Despite a flurry of activity in the run-up to the new laws, many companies don't appear to be making much effort to comply. Many attended briefings by the Privacy Commissioner and advisory firms. Some obtained template-style privacy polices from their legal advisors. This is better than doing nothing – but not by much!

Taking the next step

An effective data protection strategy is not a legal issue, it's a business issue. So what should companies do about data security and APP compliance?

- Obtain a gap analysis from an experienced consulting firm to determine current status and the gap to effective data protection and compliance
- Allocate the budget and agree on a clear program to move towards compliance. This can take one or more years depending on current status
- Start the journey towards effective data protection and as a consequence secure compliance with the APPs

We have seen little evidence so far that the new laws are making much impact on the behaviours of companies. Loop offers consulting services and advice to customers on Privacy regulations. As an example, The Loop Privacy Hub is a joint initiative with major global security vendor McAfee.

The Privacy Commissioner's decision against dating website operator Cupid is interesting. Cupid operates 35 dating sites. Security weaknesses saw the personal records (in some cases, very personal) of 254,000 Australians stolen by hackers. The commissioner dealt with the matter under the old rules so did not have access to the fines now available. He made a finding against Cupid on the basis it failed to encrypt passwords and retained customer data for too long.

The decision is complimentary of the steps taken by Cupid to correct the problems after they were discovered and the constructive way they engaged with the commissioner to close the stable door. The breach was clearly preventable and many of those affected will have thought Cupid got off lightly.

Had Cupid been caught under the new rules, perhaps a substantial fine would have been appropriate. What is unclear is whether one would have been imposed.

> Privacy and data protection rank in the top five priorities for US firms but are still well down the list in Australia

Contrast this with the breach in the United States by Target in late 2013. Millions of customer records were released onto the internet due to a security weakness in point-of-sale devices. Unlike Cupid, Target had a strong security posture and was compliant with PCI-DSS and other US regulations.

Target has spent millions (so far, in excess of US$70 million) in mandatory notifications and rectification. The CEO and CIO no longer work at the company. The share price has also been adversely affected: serious consequences for a serious breach.

These differences in regulatory approach and impact are most likely the reason why privacy and data protection rank in the top five priorities for US firms and why the same issues are still well down the list in Australia.

Another issue for data protection in Australia is the Commonwealth Government's view that data protection regulations may impose unreasonable burdens on business. Conversely, most developed nations consider that effective protection encourages business activity and they require strict compliance when dealing with customer data, particularly health data. That is not yet the case in Australia, even under the new rules.

Time to get tough

It seems clear that despite the new regulations, many Australian firms are still directing their budgets and efforts into areas other than compliance with the Privacy Act. It is early days and we should give the commissioner the benefit of the doubt, but the signs are far from encouraging. Perhaps he will need to refocus his limited resources away from education and consultation into audit and strict enforcement if data protection is to get the profile it strongly deserves.

Adam Davenport is managing director of Loop Technology in Sydney

Regulatory bodies

PCI-DSS
This scheme is administered by a group of global credit card companies and is primarily designed to reduce financial fraud. It imposes obligations on firms that wish to use credit and debit cards. As a self-regulatory regime, it has been remarkably successful in changing company behaviours and compelling changes to security and data protection. It has done so through an effective audit and enforcement processes.

APRA
The Australian Prudential Regulatory Authority was created by Federal legislation, like the Privacy Commission. It is funded by the industries it supervises. It regulates banking and the related financial services industry. APRA has comprehensive requirements designed to reduce fraud and improve security. It manages a random audit program and imposes sanctions on firms that fail to comply. Like the card companies, it has successfully changed the way its members deal with security.

ACCC
The Australian Competition & Consumer Commission is a high-profile Federal body. It has continued the powerful enforcement posture developed by Professor Allan Fels. The ACCC is not reluctant to take on large enterprises when it observes what it believes are contraventions of Australia's anti-trust and trade practices laws. Recent proceedings against Coles are a clear example.