‘Australian Privacy Principles’ (APP) 2014 regulatory changes. Is your business ready for it?

What can technology do? The new act introduces a system of 13 Australian Privacy Principles, these will have a big impact on the collection and handling of personal information both for ORGANISATIONS.

At a recent Media lunch, Pat Devlin, Country Manager ANZ at WatchGuard Technologies, shared his point of view on the latest 'Australian Privacy Principles' (APP) and how you can get reasonable measures in place that shouldn’t require a major new technology investment. LogicalTech is one of the leading & trusted Professional Partner with WatchGuard Technologies in Australia.

Overview of ‘Australian Privacy Principles’

The new upcoming privacy legislation, ‘Australian Privacy Principles’, has an immediate impact on internet security, business and government. Scheduled to be implemented from 12 March 2014, the legislation promises to be the biggest change in privacy laws in the last 25 years.

Under this new information privacy law, organisations are obligated to adopt practices and systems that will protect any personal data that they hold, which will make internet security a critical component of any organisation’s strategy. The incentive to ensure these obligations are met is essential as the penalties to non-compliant organisations will be severe ranging up to $1.7 million.

Discussion Points:

The new act introduces a system of 13 Australian Privacy Principles, these will have a big impact on the collection and handling of personal information both for ORGANISATIONS – Public and Private and INDIVIDUALS including small businesses. It also makes extended provisions of investigation and enforcement to ensure compliance and for the first time sees the introduction of a civil penalty regime for breaches of privacy.

What exactly are these penalties?

This depends very much on the type of data (credit and health information attract larger penalties) and the type of breach - larger or multiple breaches attract larger penalties. For individuals or small businesses the civil penalties go up to 2,000 penalty units which right now equals $340,000, for larger organisations fines range up to $1.7M!

There are several steps that EVERY APP Entity (defined as any person or organisation handling private data) must take before March 12 in order to be in compliance with the revised act. These include a requirement for a more proactive privacy policy around the management of personal information. A policy will need to address different categories of information and take reasonable steps to implement practices, procedures and systems that comply with the APPs.

What are you required to do?

Among other things, entities must take reasonable steps to protect personal information from 'interference', such as attacks on their computer systems. This is in addition to existing obligations to protect personal information from misuse and loss, and unauthorised access, modification and disclosure.

This idea of reasonable comes up again and again in the revised act and in the original. The real question most entities must ask themselves is, “What is reasonable for us?” The true test of this may not happen until the OIAC starts investigating their first test cases. In most cases, reasonable will relate both to the size of the entity and the sensitivity of the data. The revised act includes lengthy sections on credit and health information and the most severe penalties are associated with these data sets.

Notably absent from the revised act is any requirement for mandatory disclosure of data loss. It is strongly recommended for entities to have a disclosure policy in place but not required. This requirement however, may not be far away. Mandatory reporting amendments have received strong support including Senate Committee endorsement and are likely to be on the way some time soon.

What can technology do?

Getting reasonable measures in place shouldn’t require a major new technology investment. A privacy policy will identify what data needs to be protected and where that data is held. Some reasonable steps are simple, if data is present on laptops or removable media, then it needs to be on encrypted storage. These days, most operating systems bundle file encryption technology for free. Data moving around your organisation becomes a little trickier. Having reasonable protection of computer systems will definitely include all the basics, Firewall, IPS and Anti-Virus but will very likely also require some way to report on specific data sets as they move outside the organisation.

Many technology companies offer Data Loss Prevention tools to perform this task. These tools monitor network traffic and look for data containing things like Names, Addresses, Medicare or Credit Card numbers. The depth of scanning and reporting required for the “reasonable steps” requirement will depend on the size of the entity and the sensitivity of the data. Many security services from large international companies may not be up to the task, being geared to US or European data sets. Being able to scan for Social Security numbers won’t help an Australian entity needing to stop Medicare data loss.

WatchGuard and Data Loss Prevention

WatchGuard DLP is a uniquely comprehensive service for the WatchGuard UTM platform that helps keep private data private. It prevents data breaches by scanning text and common file types to detect sensitive information attempting to exit the network. This subscription-based service is affordable, easy to configure, and integrated into WatchGuard's award-winning XTM family of network security solutions. For a more comprehensive enterprise level solution and deeper scanning, WatchGuard offers the XCS Next-Generation Content Security Appliances which includes highly granular data loss prevention.

A built-in library of over 200 rules including AUSTRALIA and NEW ZEALAND specific filters, allows IT to quickly create and update corporate DLP policies. Rules cover personally identifiable information, financial and healthcare data, and more. All data in motion transmitted via email, web, or FTP is automatically scanned against your rule set to be sure to meet the REASONBLE measures test.

LogicalTech is one of the leading & trusted Professional Partner with WatchGuard Technologies in Australia. For all Media Inquiries please contact Cassidy Poon, National Marketing Manager for LogicalTech. LogicalTech confirms that all contact information provided will be treated confidentially and will only be used to contact you regarding this enquiry.

Contacts

Cassidy Poon
03 86436444
mailto: cassidyp@logicaltech.com.au