Protect and serve how safe is your personal data?

The revelations of the Heartbleed vulnerability in April and the recent implementation of Australia's new privacy regime in March have put data breaches firmly back in the limelight. ***Clare Coulson*** *finds out more...*

It's the information age; there's data, data everywhere. By 2020 IDC forecasts that we will generate 40 zettabytes (ZB) of data. To give you an idea of just how much data that is, American linguist Mark Liberman calculated the storage requirements for all human speech ever spoken at 42 zettabytes if digitized as 16 kHz 16-bit audio. Every minute of every day we create more than 204 million email messages, over two million Google search queries and $272,000 is spent on e-commerce. Not only is that a lot of information, but amongst it is a great deal of data that is categorised as sensitive – financial information, personal health information, personally identifiable information and trade secrets and intellectual property. And being breached.

Mega breaches and new targets

The OpenSSL Heartbleed vulnerability was a timely reminder that sensitive data is not always as secure as it should be. Symantec's Internet Security Threat Report 2014 also showed that data breaches are getting bigger. It declared 2013 "the year of the mega breach". A mega breach is a breach that exposed one or more pieces of information about more than 10 million identities. In 2012 there was only one mega breach. In 2013 there were eight. In total Symantec says over 552 million identities were breached in 2013, "putting consumer's credit card information, birth dates, government ID numbers, home addresses, medical records, phone numbers, financial information, email addresses, logins, passwords, and other personal information into the criminal underground". The total number of breaches in 2013 was 62 percent greater than in 2012 with 253 total breaches and the top types of information breached were real names, birth dates and government ID numbers (such as social security). Along with the usual targets, Symantec says that attackers are now turning to the internet of things and wearables.

"Baby monitors, as well as security cameras and routers, were famously hacked in 2013. Furthermore, security researchers demonstrated attacks against smart televisions, automobiles and medical equipment. This gives us a preview of the security challenge presented by the rapid adoption of the internet of things (IoT)," the report states.

Symantec's director of technology Sean Kopelke noted; "If we can hack Google Glass then we can actually see someone punch in their PIN."

Image: midnightrider79

Although many organisations have invested in anti-virus technology, sniffers and next-generation firewalls, security experts attending the Techleaders Forum in Queensland in February said these were no longer a guarantee of security as they generally only protected organisations from a known threat. Vendors recommended companies take a layered approach to security using a range of tools and services in order to provide themselves with the best chance of protection.

Who is sharing your information?

Last year the *Wall Street Journal* conducted a test to identify what personal information gets passed to other companies when users log in to a site. It reported that it had tested: "50 of the top sites (by US traffic) that offer registration, excluding sites that required a real-world account, such as banking sites.

The results showed that 50 percent of the sites tested were sharing some kind of data with third parties, including email addresses, names, usernames, age or year of birth, zip code or other information either in full, in part or encoded. Fifty-three percent of the sites that sent either email addresses or usernames, sent them in full.

In general the information shared with third parties was for analytics, targeted self-promotion or to serve advertising. In some cases, such as dating and networking sites, the information was also used to perform services on users' behalf.

Five of the 50 sites tested shared full, unencoded email addresses, including CNN.com, Ask.com, Pinterest, Whitepages and the Wall Street Journal itself. Another five shared partial or encoded email addresses. CNN and the Whitepages responded to the Journal saying they were investigating while Pinterest and Ask.com said they no longer practice this. The WSJ.com said most of its personally identifiable information detected was transmitted in error and that it is working to close that hole.

Those sites that pass on the most data fields can be seen as instrumental in leaking sensitive information – even anonymous data can be gathered and later paired with email addresses from other sources to reveal the behaviour of a named person for more targeted advertising purposes.

A/NZ by the numbers

In his keynote speech Federal Attorney General, Senator George Brandis told the Cebit conference in Sydney in May that cybercrime was now costing Australia over $1 billion a year. He said that although IT was a key enabler of business and all aspects of modern life it was "unfortunately also a key enabler of crime and security threats". In a separate Cebit speech Joe Franzi, assistant secretary cyber security at the Australian Signals Directorate, confirmed that attacks were on the rise, with reports to the Cyber Security Operations Centre up from 1259 in 2011 to 2168 last year. He said mining and resources, energy, defence, technology and financial sector organisations were at greatest risk.

In New Zealand the 2013 annual report from the Office of the Privacy Commissioner showed a sharp increase in the number of data breaches being voluntarily reported. While such reporting remains voluntary in New Zealand the Office of the Privacy Commissioner has recently started to track breach notifications more formally. In 2012-13 there were 107 breaches reported, only 23 of which came from the private sector. Government, hospitals and other health agencies reported the most breaches. Interestingly the data also shows that the largest number of breaches seemed to come down to human error, with ' Electronic information sent to wrong recipient ' and 'Physical information sent to wrong recipient' being the most frequent cause of breaches, followed by website problems. Only four instances of data breach were caused by hacking in 2012-13. However, because breach reporting is entirely voluntary at present the Privacy Commission's figures are unlikely to reflect the actual number of breaches that occur and who they are happening to, with many private companies likely reluctant to broadcast such information.

"On March 12 Australia implemented its new privacy regime; the most significant shakeup in its privacy laws in over two decades."

A new regime

On March 12 Australia implemented its new privacy regime; the most significant shakeup in its privacy laws in over two decades. The 13 new Australian Privacy Principles (APPs) replace the previous 10 National Privacy Principles and affect Government departments, most private enterprises and not-for-profit organisations.

To be compliant organisations have to have processes and technology in place to allow access to information not just on corporate CRMs for example, but also information collected from emails or social networks. The onus is now on businesses and other organisations to protect the information and privacy of their clients. To achieve this APP 1 requires entities to consider a 'privacy by design' approach to systems and procedures, and embed

Australian Privacy Principles — a summary

The Office of the Australian Information Commissioner has put together a summary of the new Australian Privacy Principles for private sector organisations, Australian Government and Norfolk Island agencies covered by the Privacy Act 1988. It, along with other information, can be found at: http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/app-quick-reference-tool

privacy protections in the design of their information handling practices. Compliance will help to establish an organisational culture and processes that will assist with compliance with all the other APPs.

At the very minimum these organisations need to have a clearly defined and well-publicised policy regarding data management and ensure that staff understand and comply with that policy. The new rules also require much more transparency on the part of large organisations which use personal data so consumers receiving direct marketing materials can now find out more about what information is being held and how it is being used.

A whitepaper by Hitachi Data Systems, says that data quality and integrity are paramount for a successful privacy programme. It says that entities affected by the new regime will need to ensure that any customer data that is to be retained, whether it is structured data in a CRM or unstructured data in emails, log files or social media, needs to be managed in an "immutable, auditable and versioned" manner. This means the data needs to be protected, copied and searchable.

According to law firm Corrs Chambers Westgarth, even foreign companies conducting activities in Australia are subject to the new Principles. And their activities outside Australia are covered by the Act, if:

a) they "carry on business in Australia"; and
b) they collect or hold personal information in Australia.

This is the case even if they have no physical premises in Australia but a web presence that collects the personal information of people who are physically in Australia. A foreign company will also find that if it enters a transaction with an Australian organisation that involves the transfer of personal information from Australia to the foreign company, the Australian organisation will seek a contractual obligation by the foreign company to uphold the APPs.

The missing piece

Although the new privacy rules in Australia have created penalties of up to $1.7 million for enterprises which fail to properly protect data, they stop short of requiring that data breaches be disclosed as they are in the USA.

In New Zealand disclosure also remains voluntary, however, in its 2011 review of New Zealand privacy legislation the Law Commission recommended that New Zealand needs to move to mandatory breach reporting in cases of serious breaches – something the Office of the Privacy Commission is publically supportive of.

Until such requirements are law, however, it is likely that there will not be enough incentive for proper data protection and disclosure by the corporate sector in particular for fear that such revelations may do more damage than good. And with estimates that the Target credit card hack in the lead up to last Christmas cost the company more than $500 million and wiped 10 percent off its market capitalisation one can see why.