Inhouse Counsel

2017 . Vol 21 No 5

Contents

page 94 **General Editor's note**
Caterina Cavallaro *SYDNEY WATER CORPORATION*

page 95 **Who are you and how can you prove it? The evolving requirements for verification of identity rules**
Nikki Robinson *and* ***Angus Roy*** *CLAYTON UTZ*

page 99 **FIRB 2017 — changes under Australia's foreign investment regime**
Katherine Yang *and* ***Malcolm Brennan*** *KING & WOOD MALLESONS*

page 102 **Caution: indemnity ahead — Court of Appeal overturns decision in favour of CSR in CSR Ltd v Adecco (Australia) Pty Ltd**
Scott Alden *and* ***Victoria Gordon*** *HOLDING REDLICH*

page 105 **404 error: cyber security for business**
Daniel Coster *KOTT GUNNING LAWYERS*

page 108 **Media buying: contracting tools to create transparency**
Simone Brandon *AUSTRALIAN ASSOCIATION OF NATIONAL ADVERTISERS*

page 111 **Alliances, PPPs and delivery partner contracts — general update and tips**
James Forrest *KING & WOOD MALLESONS*

Information contained in this newsletter is current as at July 2017

LexisNexis® Butterworths

General Editor's note

Caterina Cavallaro *SYDNEY WATER CORPORATION*

In this edition of *Inhouse Counsel*:

- The rise of identity theft and fraud, together with the increased popularity of digital signatures and e-contracts, means that it is more important than ever to be able to prove who is signing a contract. Nikki Robinson and Angus Roy (Clayton Utz) take us through the newly introduced verification of identity, including what you need to know as in-house counsel and how to comply with the new requirements.
- Katherine Yang and Malcolm Brennan (King & Wood Mallesons) review the changes under Australia's foreign investment regime, focusing on the recently established Critical Infrastructure Centre and its register. The article discussed the key benefits of the new changes and identifies issues to keep in mind for clients seeking Foreign Investment Review Board (FIRB) approval.
- Indemnities are complex, have far-reaching consequences and are often not properly understood. Scott Alden and Victoria Gordon (Holding Redlich) summarise the key issues in a recent NSW Court of Appeal decision, *CSR Ltd v Adecco (Australia) Pty Ltd*,[1] highlighting the perils of a poorly drafted indemnity.
- In a timely consideration of cyber security, Daniel Coster (Kott Gunning Lawyers) discusses ransomware and its origins, considers Australian and global examples, and reviews the Australian legislative framework. The article considers the Privacy Act 1988 (Cth) and the recently introduced protections which will come into effect in 2018.
- Simone Brandon (Australian Association of National Advertisers) (AANA) considers the AANA's Media Contract Template and Media Contract Guidance Notes, both of which help advertisers obtain greater transparency over the return and effectiveness of their media investment.
- In recent years, alliances and public private partnerships have remained popular delivery alternatives for major projects, while the delivery partner model has emerged as a further option to assist with project delivery. James Forrest (King & Wood Mallesons) compares the different delivery alternatives and identifies key issues to consider when working with these models.

Caterina Cavallaro
Senior Legal Counsel
Sydney Water Corporation
caterina.cavallaro@sydneywater.com.au
www.sydneywater.com.au

Footnotes

1. *CSR Ltd v Adecco (Australia) Pty Ltd* [2017] NSWCA 121; BC201704057.

404 error: cyber security for business

Daniel Coster *KOTT GUNNING LAWYERS*

The commercial internet is a relatively recent development. With the proliferation of faster and cheaper technologies, we are now heavily dependent on internet-connected devices for both business and pleasure.[1] With new technologies come new risks, and even large multinational businesses have fallen victim to cyber attacks and lost valuable commercial information.

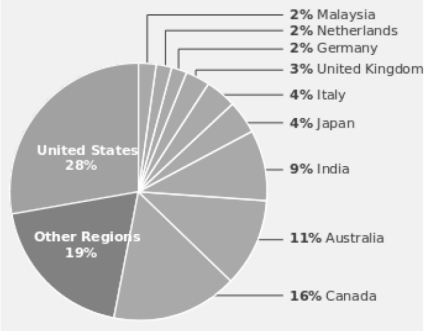
A breach of digital security, whether or not private data is compromised, can result in reputational damage and loss of business. Businesses may seek to minimise such loss by not publicly disclosing cyber attacks or downplaying the extent of any breach. This article examines the legal obligations for Australian businesses to disclose cyber security breaches, as well as the importance of taking a proactive approach to cyber security generally and when responding to a breach of personal information in particular.

The threat

In 2005, the world first experienced the unprecedented threat of ransomware. In short, ransomware is the criminal misuse of data encryption software (designed to secure private data from unauthorised access). Ransomware can be activated by simply opening an infected file in a seemingly innocuous email. Once activated, the ransomware encrypts all the files on your device, preventing access until a ransom is paid for the "key" to decrypt the data. It is estimated that between October and December 2013, over US$27 million had been paid in ransoms as a result of one type of ransomware alone (CryptoLocker).[2] From January 2015 to April 2016, Australia accounted for 11% of global ransomware infections, more than the UK, Germany and Italy combined.[3]

In 2013 and 2014, internet service company Yahoo! suffered two major embarrassing data breaches, affecting around 1.5 billion customer accounts. The breaches are currently considered to be the largest in the history of the internet. Stolen data is understood to have included customers' names, email addresses, telephone numbers, dates of birth and encrypted passwords. Yahoo! was in the process of being sold, with a substantial price agreed upon, when the breaches were (belatedly) publicly disclosed in 2016. The sale price was subsequently reduced by US$350 million. Yahoo!'s delay in disclosing the breaches attracted significant media attention, with affected customers at risk of identity theft and other crimes for 3 years. Yahoo! is a cautionary tale. Their handling of the breaches resulted in the loss of a substantial number of advertisers (a key revenue source) and customers.

Ransomware infections by region, January 2015 — April 2016



Source: Symantec, *An ISTR Special Report: Ransomware and Businesses 2016*

In July 2015, a website for cheating spouses, Ashley Madison, experienced a massive data breach. A group of hackers stole customer data including names, residential addresses, credit card records and user search histories. When the site failed to obey a demand by the hackers to shut down, the group released the data publicly, along with a significant number of corporate emails it had also stolen. A class-action lawsuit by customers is currently being prepared in Canada as a result of the breach.

Legislative framework

The Privacy Act 1988 (Cth) (the Act) regulates the storage and use of personal information by many (but not all) private sector organisations.[4] The definition of "organisation", for the purposes of the legislation, includes an individual, body corporate, partnership, unincorporated association, or a trust (but not a small business operator, subject to certain exceptions).[5]

Australia's data protections laws have been significantly updated with amendments to the Act made by the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) and the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth).

Enhanced protection

The Privacy Amendment (Enhancing Privacy Protection) Act introduced amendments in the form of the 13 Australian Privacy Principles (APPs), imposing more stringent privacy obligations on organisations as to the protection, disclosure and management of personal information. The principles seek to ensure organisations manage personal information openly and transparently, such that customers are aware of how their information is being used and their rights with regard to the same. By now, readers would be familiar with these principles, with them having been in effect since March 2014.

Data breaches

The Privacy Amendment (Notifiable Data Breaches) Act is a significant amendment to the Act, taking effect from February 2018. The Act now imposes a requirement on organisations to provide notification of certain breaches of data security, termed an "eligible data breach". An eligible data breach occurs when either:[6]

- there is unauthorised access to, or disclosure of, information that a reasonable person would consider likely to result in serious harm to any affected individuals; or
- information is lost in circumstances where the above is likely to occur.

In the event of a data breach, organisations have notification obligations under the Act.[7] The obligation to notify of a breach arises where an organisation is aware that there are reasonable grounds to believe there has been an eligible breach. If an organisation suspects there may have been an eligible breach, the Act requires the organisation to expeditiously carry out an assessment to determine whether there are reasonable grounds to believe the relevant circumstances amount to such a breach.[8] An organisation is required to take all reasonable steps to have such assessment completed within 30 days of becoming aware of the potential eligible breach.

Where there are reasonable grounds to believe an eligible breach has occurred, the Act requires an organisation to prepare a statement setting out particulars of the breach, including the nature of the information concerned and recommendations for individuals affected by the breach.[9] The statement must be provided to the Privacy Commissioner as soon as practicable. The organisation is also required, if practicable, to take reasonable steps to provide notice of the statement to each affected individual. If that is impracticable, the organisation is required to publish the statement on their website and to take reasonable steps to publicise the contents of the statement.

Role of the regulator

The Office of the Australian Information Commissioner (OAIC) is the regulatory body responsible for administering Australia's privacy laws and handling privacy complaints. The OAIC has published a privacy regulatory action policy, which provides guidance as to the action it will take when a breach of privacy occurs.[10]

Relevantly, the OAIC's preference is to work with business to ensure legal compliance, rather than being a purely punitive body. If a business acts in good faith and is candid with the OAIC, assistance will generally be provided. This is of course subject to various factors, including the seriousness of any breach, whether the business has been the subject of prior regulatory action (ie whether they are a "repeat offender") and any deterrent value (generally and for that business specifically) in taking punitive action.

The OAIC also provides a helpful online guide on handling privacy breaches,[11] which outlines the key areas businesses need to focus on to protect personal information and what to do in the event of a breach.

Implications for business

It is essential to ensure organisations are aware of their new obligations under the Act. The amendments to the Act impose a positive requirement to investigate potential breaches of data, and to then report any eligible breach to the Commissioner and any affected individuals.

The specific message for businesses is that, while a breach of digital security can be embarrassing and financially damaging, the new legislative framework introduces more rigorous obligations of transparency and accountability. With the rise of cloud-based storage in particular, and an increase in reliance on technology more generally, businesses need to have an ongoing focus on cyber security, in terms of both prevention and when responding to a breach.

The general message is that the pace of change in this area is increasing, and businesses need to be both vigilant and proactive. Indeed, it is no longer sufficient to only be aware of Australian legislative changes. Businesses wanting to operate, or provide goods or services, in the European Union (EU) will also be affected by compliance requirements in the EU's General Data Protection Regulation from May 2018.

While regulation in this area is developing rapidly, it is almost inevitably outpaced by evolving technologies and emerging threats. As the ransomware graph above demonstrates, Australia is at the forefront with these risks.

Daniel Coster
Associate
Kott Gunning Lawyers
dcoster@kottgunn.com.au
www.kottgunn.com.au

Footnotes

1. According to 2013–14 Australian Bureau of Statistics (ABS) data, 94.7% of businesses had internet access, 47.1% had a web presence and $267 billion of income was generated annually from online customers — see Australian Bureau of Statistics, *Business Use of Information Technology and Innovation in Australian Business*, 15 June 2017, www.abs.gov.au/ausstats/abs@.nsf/mf/8166.0.
2. See V Blue, *CryptoLocker's Crimewave: A trail of Millions in Laundered Bitcoin*, 22 December 2013, www.zdnet.com/article/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin/.
3. Symantec *An ISTR Special Report: Ransomware and Businesses 2016* (19 July 2016) www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf.
4. Pursuant to amendments by the Privacy Amendment (Private Sector) Act 2000 (Cth).
5. Privacy Act 1988 (Cth), s 6D.
6. Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth), s 26WE.
7. Above n 6, Subdiv B.
8. Above n 6, s 26WH.
9. Above n 6, s 26WK.
10. Office of the Australian Information Commissioner, *Privacy Regulatory Action Policy*, June 2015, www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/.
11. Office of the Australian Information Commissioner, *Data Breach Notification — A Guide To Handling Personal Information Security Breaches*, August 2014, www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches.