Carter Newell LAWYERS

Cyber Risk Newsletter

September 2017

Cyber update - what's going on

Katherine Hayes, Special Counsel
Greg Stirling, Senior Associate

Data breaches are occurring more frequently, and with the new mandatory data breach reporting obligations looming, it's important to understand the nature of the risk so that lessons can be learned.

Inadvertent breach - Boeing

Perhaps the best example of an inadvertent breach is a Boeing employee's breaching of 36,000 fellow-employees' personal data in the United States. The unfortunate employee had emailed a spreadsheet to his spouse for help with a formatting issue. He did not realise that there was sensitive personal information contained in hidden columns of the spreadsheet, including names, addresses, dates and places of birth and social security numbers. Boeing's investigations confirmed that the data was not accessed or passed on to anyone else by either the employee or his spouse.

The threat was therefore contained, and the risk of harm very low.

Boeing notified the relevant authorities, investigated the breach, notified each of the 36,000 affected individuals offering complimentary identity monitoring for two years. A conservative estimate of the cost of the identity monitoring at $10 per person per month puts the total cost of the monitoring alone at over $8 million. Boeing would also have incurred the costs of the investigation, notification and crisis management.

The inadvertent disclosure could potentially have been avoided through additional staff training and implementation of software such as, ironically, the Cipher application sold by Boeing which '*ensures hidden information is not inadvertently included in and transmitted with a file*'.

Australia's largest data breach so far - Red Cross

In August this year, the Office of the Australian Information Commissioner (**OAIC**) released its report into the Red Cross data breach, which is Australia's largest to date.

550,000 Red Cross blood donors' personal information was breached when an unsecured back-up copy of the information was inadvertently posted to a publicly accessible location online by a third party provider.

The personal information was provided by donors when they completed Red Cross' online blood donation eligibility form between 2010 and 2016, and included identifying information such as names, addresses and dates of birth as well as details of any '*at risk*' sexual behaviour, or recent pregnancies.

After the breach, there were reports that the affected donors were being targeted by '*SMiShing*', which is a text message containing a link to a false site tricking victims into providing further sensitive information.

The breach wasn't discovered by the Red Cross, but was discovered by an unrelated third party and notified to AustCert, of which Red Cross was an existing client. It is still unknown how widely the leaked data has been distributed.

The OAIC report praised Red Cross' handling of the event, but issued a reminder to organisations that privacy obligations cannot be outsourced, and that:

> *…all organisations must put into place reasonable measures to ensure their third party providers' compliance with appropriate privacy and data security practices and procedures.*

Both Red Cross and the third party provider have given enforceable undertakings to the OAIC.

This breach is another example of the '*sticky*' nature of the privacy obligations, which cannot be avoided through the use of third party providers.

Business interruption - DLA Piper

In June 2017, international law firm DLA Piper was one of many victims of the global cyberattack by Petya (one of its many names). While the attack reportedly originated in an overseas office of the firm, the Australian offices were impacted. The firm's email, telephone and network systems were offline. DLA Piper reported that there was no evidence of unauthorised access to client data or other confidential information.

While the firm was apparently unable to contact some of its clients directly, it posted regular updates on its websites, and reportedly communicated with its staff by text message, apparently successfully implementing an incident response plan.

By all reports DLA Piper handled the breach as well as could be expected, but presumably would have suffered business interruption losses as a result of the inaccessibility of its systems.

Contracts with third parties - FedEx – TNT

Another high-profile local victim of Petya was TNT Express, which is part of FedEx. For over a week TNT Express' Australian operations and communications systems were reportedly affected, and TNT Express was unable to perform its essential function of delivering its customers' packages.

Some customers took to social media to vent their frustration about the delays, and TNT Express' communication with them, further damaging the company's reputation. This is a good example of how international threats which may not have an Australian focus may still impact local businesses which are part of a global entity or group of companies.

Rogue employee – Bupa

Almost 20,000 Australian customers of Bupa had their personal data leaked by a rogue employee based in Bupa's UK office. The leaked data included names, dates of birth and contact details, and was part of a large leak of over 500,000 records released by the disgruntled employee. No financial or medical information was leaked, but the incident has proven to be a high-profile headache for Bupa, and a reminder of the threat that can lurk within.

Lessons learned

Data breaches can take place anywhere, at anytime, and are difficult to guard against. It is important to be on the front foot when considering the risk.

These incidents can teach us that:

1. Liability under the Privacy Act cannot be avoided by delegating to third parties;
2. An inadvertent breach can be just as harmful as a malicious attack;
3. It is important to have incident response plans in place;
4. The handling of a breach is vital in containing the damage; and
5. Beware of rogue employees.

Authors

Katherine Hayes
Special Counsel

P: +61 (0) 7 3000 8349
E: khayes@carternewell.com

Greg Stirling
Senior Associate

P: +61 (0) 7 3000 8366
E: gstirling@carternewell.com