Carter Newell LAWYERS

Cyber Risk Newsletter

March 2016

INSURANCE

CONSTRUCTION & ENGINEERING

RESOURCES

CORPORATE

COMMERCIAL PROPERTY

LITIGATION & DISPUTE RESOLUTION

AVIATION

Cyber risk update: recent security breaches

Katherine Hayes, Senior Associate

Greg Stirling, Associate

2015 heralded a sudden increase in high profile cyber security breaches of companies with a presence in Australia. 2016 has continued that trend. The reputational risks are potentially significant, and companies are having to prepare for an increasing and ever-evolving threat.

We outline below some of the more high-profile cyber security breaches from late 2015 / early 2016.

Patagonia Clothing Company

In September 2015, hundreds of customers of outdoor clothing company Patagonia may have had their bank details stolen after hackers breached its Australian website. The company said that credit and debit card details from 600 customers who used the site to purchase goods between 4 August and 12 September 2015 may be *'at risk'*.

A further 12,500 customers may have had less sensitive data compromised, such as names, email addresses, account passwords and possibly mailing addresses. The website was disabled for one month which would have affected online sales, and customers were reportedly offered one year of complimentary credit monitoring.

Kmart

In October 2015, Kmart's online operations were hacked in a security breach that exposed customers' personal information. The data stolen was limited to customers' names, email addresses, delivery and billing addresses, telephone numbers and product purchase details. No credit card data was stolen. Kmart issued a media release stating that *'immediate action was taken to stop any further information being accessed'* as soon as the breach became known.

David Jones

Also in October 2015, David Jones' computer system was hacked and the personal details of some of its customers stolen. No credit card information or passwords were taken, and once it discovered the issue David Jones moved quickly to prevent any further incident. David Jones received wide-spread media coverage of the breach, with interest heightened by the contemporaneous Kmart breach.

Aussie Farmers

In November 2015 thousands of customers of Aussie Farmers Direct had their personal information posted online as a result of a hacking attack. The food delivery company was the target of an extortion attempt by hackers, who demanded an unusually high six-figure ransom before posting the information of more than 5,000 customers online.

The information included names, addresses, phone numbers and email adresses of former and existing customers. Aussie Farmers Direct says it has increased its security measures and is working with *'its banking partners, the Office of the Australian Information Commissioner and IT security experts'* in taking steps to avoid another breach.

Queensland TAFE

In November 2015 more than 600 Department of Education records, dating back to 2013, had been accessed illegally, although financial data had not been breached. A ransom of 26.81 Bitcoin (approximately $15,000) was demanded for not releasing the information. The ransom was reportedly unpaid.

While the government said that the information that was breached was mainly *'low-level'* information, some *'sensitive, personal information'* concerning children had been breached, including details of bullying and sexual assault complaints.

Optus

In November 2015, an employee of ARC Mercantile, a debt collection agency used by Optus to assist in recovering outstanding debts, posted approximately 31,140 Optus customers' personal and credit history information on the website freelancer.com. The employee apparently wanted to engage a freelance contractor to analyse the data on a spreadsheet, which contained personal information including customers' names, contact details, addresses and debt collection histories.

Upon learning of the incident from a user of the website, Optus reportedly:

- Asked freelancer.com to remove the posting;
- Began an investigation to reveal the source of the disclosure;
- Commenced legal proceedings against freelancer.com to ascertain the identity of the individuals who may have accessed the information. It emerged that 51 potential freelance contractors may have accessed the information;
- Notified the Office of the Australian Information Commissioner (**OAIC**) of the disclosure; and
- Wrote to the individuals who had downloaded the spreadsheet, advising them that the disclosure of information was unauthorised and requested that they destroy any record they have of the information.

Royal Melbourne Hospital

In January 2015, a virus infected the computers across the Royal Melbourne Hospital. The virus reportedly impacted the pathology department, meaning that processing blood, tissue and urine specimens needed to be done manually rather than with the assistance of the computer network. The radiology department was also impacted and the hospital was apparently forced to send its major trauma patients to other hospitals.

Media coverage of the incident was widespread and it is not presently clear whether the security of patients' records was jeopardised.

Potential costs of the incidents

The breached entities were faced with an unfamiliar situation and were exposed to a number of losses and liabilities including:

- Credit monitoring costs - affected persons are often offered such a service for up to 12 months after a breach;
- Crisis management and PR costs;
- IT security costs to ascertain the extent of a breach;
- The cost of upgrading security systems and computer networks;
- The costs of notifying the OAIC and affected customers and any subsequent dealings;
- Business interruption costs; and
- Possible liabilities, such as liability for losses arising out of misuse of credit cards or losses suffered by a supply-chain partner as a result of the business interruption.

In addition, the reputational damage that can arise from a data breach is more difficult to ascertain and often depends on the entity's initial response. It is clear that with the increasing media coverage reputational damage can be significant.

In statements released following the Kmart, David Jones and Optus data breaches, the OAIC praised the entities for quickly notifying affected individuals as well as the OAIC of the incident. The OAIC considers notification to be a key mitigation strategy which can potentially benefit both the affected individuals as well as the entities themselves as steps can be taken to contain damage. In light of these comments, and with the proposed mandatory data breach notification legislation expected to receive bipartisan support, it seems appropriate for entities to now consider breach notification to be an important part of their response plans.

OAIC's data breach response guide

The OAIC's guide provides four key steps to responding to a data breach, namely:

- Containing the breach and undertaking a preliminary assessment. This step is vital in ascertaining the precise nature of the incident, which will assist in determining an entity's response.
- Evaluating the risks associated with the breach (e.g. risks to the individuals affected and the risk to your organisation) so that the extent of the damage can be ascertained;
- If appropriate, notifying the breach to affected customers, law enforcement agencies and the OAIC. As discussed above, notification can assist in mitigating damage; and
- Taking steps to prevent future breaches.

With the increasing threat of cyber incidents, companies face a heightened risk of loss and liabilities arising out of data breaches. In addition, the reputational losses can be significant. Preparation and an appropriate rapid response is crucial in these circumstances.

Authors

Katherine Hayes
Senior Associate

P: (07) 3000 8349
E: khayes@carternewell.com

Greg Stirling
Associate

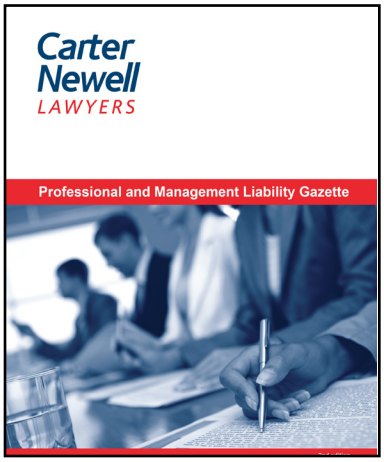
P: (07) 3000 8366
E: gstirling@carternewell.com

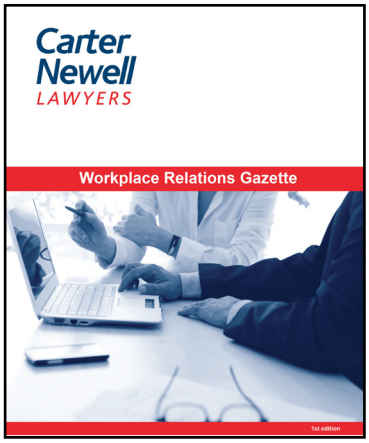
Recent Publications

Professional and Management Liability Gazette 2nd edition

The Professional and Management Liability Gazette 2nd edition is designed to provide the insurance industry with a practical synopsis of noteworthy cases concerning claims under Professional Indemnity, Directors' & Officers', and Management Liability policies and focuses on decisions that have involved procedure, brokers, solicitors and barristers, and policy interpretation.

As a premier legal service provider with one of the largest insurance practices in Australia, we are confident you will find our Professional and Management Liability Gazette 2nd edition a helpful resource.





Workplace Relations Gazette 2nd edition

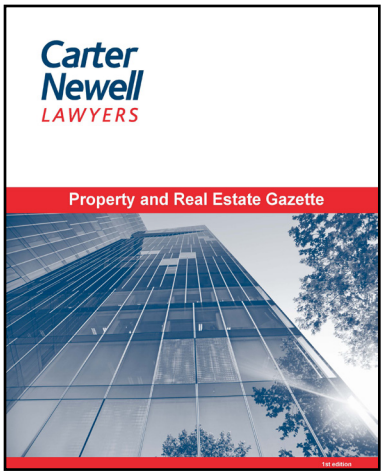
The Workplace Relations Gazette 2nd edition provides employers with a synopsis of practical and noteworthy cases with a focus on unfair dismissal, bullying, adverse action, breach of contract, general protections, penalties and sentencing, and work health and safety.

This edition of the Gazette has been created by our specialised industrial and workplace relations team.

Property and Real Estate Gazette 1st edition

The inaugural Property and Real Estate Gazette 1st edition provides useful, practical and current information to the property and insurance industries and focuses on cases related to the formation of contracts, intention to create legal relations, misleading and deceptive conduct, negligence/ bodily injury, planning and environment reform, planning law, sale and purchase contracts and valuer's liability.

Joining Carter Newell's extensive suite of publications, this Gazette has been created by our commercial property practice in consultation with our internationally recognised insurance practice.



To view a copy of these gazettes, or any of our other publications, please visit www.carternewell.com.

Brisbane
Level 13, 215 Adelaide Street
Brisbane QLD Australia 4000
Phone +61 7 3000 8300

Sydney
Level 6, 60 Pitt Street,
Sydney NSW Australia 2000
Phone +61 2 9241 6808

All correspondence to:
GPO Box 2232, Brisbane QLD 4001
www.carternewell.com
ABN 70 144 715 010