YELDHAM PRICE O'BRIEN LUSK

CYBER 'SNAP SHOT'

Background

Our increasing reliance on technology brings with it a new and dramatic front in the risk of doing business. This risk has in turn created a challenging exposure for corporate Australia and its insurers.

The frequency and complexity of cyber attacks has increased dramatically in recent years. As reliance on technology grows the incidence of cyber attacks will also increase.

The estimated annual costs of cyber attacks and data breaches to the global economy is expected to exceed $2 trillion by 2019, increasing to almost four times the estimated cost of breaches in 2015.[1]

The significance of the risks of cyber attacks saw the creation of the Australian Government's Australian Cyber Security Centre (**ACSC**) in November 2014.[2] In its first unclassified 'threat report' for 2015, ACSC reported that the cyber threat to Australia is 'undeniable, unrelenting and continues to grow'.

More recently, the Prime Minister announced the Government's 'Cyber Security Strategy' (**the CS Strategy**), a blueprint for keeping Australia 'safe and competitive in an increasingly digital world'. The CS Strategy included a promise of over $230 million invested in 33 new initiatives to improve the nation's cyber security.[3]

What are Cyber Attacks?

Cyber attacks can include crimes directed at computer technology (such as hacking) and crimes where computers are an integral part of an offence such as online fraud or identity theft.

Cyber attacks can originate from:

- malicious attacks from hackers;
- non-malicious failure such as an IT failure or the mere loss of a computer by an employee;
- IT providers both internal and external to an organisation;
- virus infections;
- breaches arising out of incorrect procedures used to host or 'cloud' services;
- 'phishing' exercises, the process of using carefully crafted emails to entice a user to click on a link or open an attachment;
- malicious use of remote access tools that allows access to a computer from a remote location; and
- 'ransomware', extortion through the use of malware that can lock a computer's content and require victims to pay a ransom to regain access.

---

[1] Juniper Research Ltd, 'The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation', Media Release, 12 May 2015.

[2] ACSC brings together existing cyber security capabilities across Defence, the Attorney-General's Department, the Australian Security Intelligence Organisation, the Australian Federal Police and the Australian Crime Commission in a single location.

[3] Launch of Australia's 'Cyber Security Strategy' Malcolm Turnbull MP, 21 April 2016.

What damage can be caused?

Potential damages may include:

- theft of intellectual property and confidential information;
- theft of personal and financial information from customers;
- data and software damage;
- direct financial loss (hackers steal funds from bank accounts or extort funds);
- investigation, notification and response costs;
- liability for third party claims from customers, suppliers or regulators;
- business interruption and loss of profits; and
- damaged reputation.

Australian examples

Daily media reports document and highlight the increasing incidents of cyber attacks. The ACSC's report detailed, however, that the incidents reported are merely 'the tip of the iceberg'. Some recent public Australian cyber attacks include:

David Jones & Kmart

In October 2015, David Jones and Kmart were left exposed after hackers stole their customers' private email addresses, home addresses and phone numbers. No passwords, credit card or financial data was lost.

David Jones and Kmart volunteered information about the breach to its customers and the Federal Privacy Commissioner.

The retailers also warned customers not to fall prey to 'phishing' attempts, advising they would not request customers to provide financial details over the phone or email.

Hyatt Hotels

In mid 2015, cyber thieves infiltrated the hotel chain's payment system and collected the credit card details of many of its customers. The hotel giant published details of the breach and encouraged its customers to review their credit card statements closely and report any unauthorised chargers to their card issuer.

International examples

Ashley Madison – Canada

In July 2015, Ashley Madison, the online dating website for married people (with the tag line 'Life is short – have an affair') was compromised. Hackers copied personal information about the site's user base and threatened to release users' names if the site was not shut down. The hackers later leaked details of approximately 36 million users of the site.

The breach has resulted in legal action with multiple class actions filed in Canada and the USA.

Target - USA

In late 2013, the retailer, Target was the victim of a massive data breach that affected as many as 110 million customers. Cyber attackers installed malicious software on point of sale devices at Target stores and were able to steal the financial information of 40 million customers and the personal information of 70 million customers. From class actions to fines, to the costs of offering free credit monitoring and hiring computer forensic investigators, the breach caused massive damages.

Regulatory Framework

The following government organisations have published guides on data breach and cyber risk:

- Office of the Australian Information Commissioner (**OAIC**);
- Australian Investment and Securities Commission (**ASIC**);
- Australian Prudential Regulation Authority (**APRA**);

- Australian Cybercrime Online Reporting Network (**ACORN**); and
- Australian Cyber Security Centre (**ACSC**).

Under the *Privacy Act 1988* (Cth) (**the Act**), agencies and organisations are required to take 'reasonable steps' to protect the personal information they hold from misuse, interference or loss and from unauthorised access or disclosure.

Apart from certain obligations under the *My Health Records Act 2012* (Cth), notification of a personal data breach is currently voluntary.

The OAIC encourages agencies and organisations to voluntarily put in place reasonable measures to deal with data breaches, including the preparation and implementation of a 'data breach policy and response plan'.

Changes are looming with the Federal Government announcing a public consultation period on the draft *Privacy Amendment (Notification of Serious Data Breaches) Bill* 2015 (**the Bill**). If the Bill passes, agencies and organisations which are subject to the Act will be required to notify the OAIC and affected individuals of serious data breaches.

In addition, with the recent publication of the CS Strategy, other changes are likely to follow. An Assistant Minister for Cyber Security and a special Adviser to the Prime Minister on Cyber Security will be established. The Government is also calling to co-design with the private sector, national guidelines for promoting good practice to improve cyber security resilience.

ASX 100 companies will be able to improve their cyber security though voluntary governance health checks that will be tailored to industry size and sector. In addition, the Government will support some 5000 small businesses to have their cyber security tested by certified practitioners.

Insurance

Traditional business policies (property damage and business interruption, commercial crime, directors and officers, public and product liability, professional indemnity and property damage) cover some losses in respect to cyber attacks and data breaches, but not all. With the increasing frequency of cyber attacks, many insurers are introducing:

- exclusions concerning cyber risks to their traditional policies; and
- specific stand alone insurance for cyber risks and privacy protection. Coverage includes both first party and third party losses.

First party losses

- privacy breach costs (investigation and notification costs, including retaining an accountant, legal advisor, public relations consultant or other third party to conduct computer forensic analysis, ensure compliance with privacy regulations, contact regulators, notify affected individuals, manage a public relations campaign, procure credit monitoring services and call centre services to handle customer inquiries);
- digital asset replacement expenses;
- business income loss;
- cyber extortion expenses and extortion payments; and
- reward payments.

Third party losses

- costs of regulatory proceedings; and
- claims by third parties (including breach of privacy, infringement of intellectual property, theft of personal or financial information and defamation proceedings).

Increased security, early detection and risk management

Whilst the Insurance industry is tailoring policies to address the emerging cyber risk exposures, the potential for cyber attacks to cause catastrophic losses and the experience to date, should focus attention on risk management to avoid such outcomes, including:

- education and awareness (preparing company wide security policies and procedures and education and training of all personnel);
- formal prevention measures to guard data security (developing a prevention plan and implementing security measure (as basic as upgrading password protection and a mainstream approach requiring passwords to be changed and updated regularly));
- early detection; and
- management and mitigation of loss (drafting and preparing a data breach response plan).

April 2016

This article was prepared by Harriet Price, Senior Associate and Paul O'Brien, Director.

Paul O'Brien can be contacted 02 9231 7020 or at pobrien@ypol.com.au and Harriet Price can be contacted on 02 9231 7050 or at hprice@ypol.com.au)

LEVEL 2, 39 MARTIN PLACE
SYDNEY NSW 2000

DX 162 SYDNEY

T: +61 2 9231 7000
F: +61 2 9231 7005
WWW.YPOL.COM.AU

YPOL PTY LTD TRADING AS
YELDHAM PRICE O'BRIEN LUSK
ACN 109 710 698

LIABILITY LIMITED BY A SCHEME APPROVED UNDER PROFESSIONAL STANDARDS LEGISLATION. LEGAL PRACTITIONERS EMPLOYED BY YPOL PTY LIMITED ARE MEMBERS OF THE SCHEME