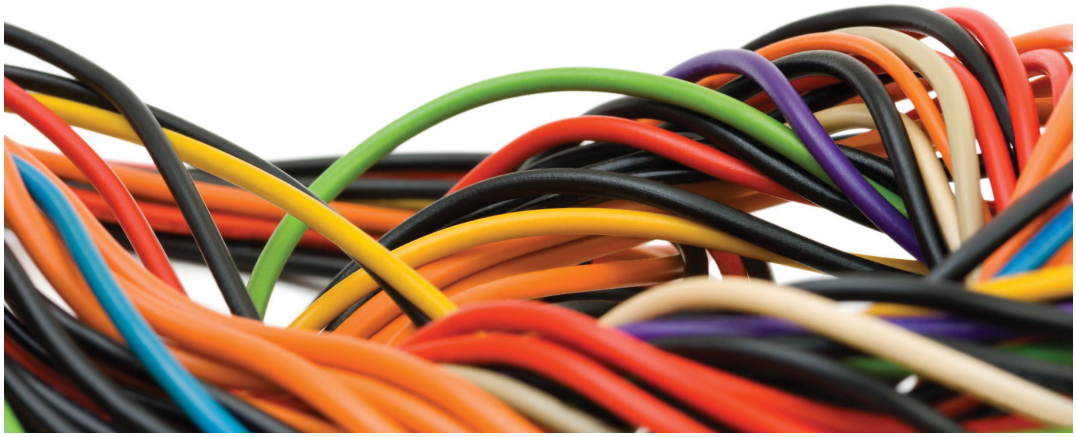
Carter Newell LAWYERS

Insurance Newsletter

May 2015



INSURANCE

CONSTRUCTION & ENGINEERING

RESOURCES

CORPORATE

COMMERCIAL PROPERTY

LITIGATION & DISPUTE RESOLUTION

AVIATION

Cyber risks update – what's going on?

Katherine Hayes, Senior Associate

Greg Stirling, Associate

Most people are aware of the headline grabbing, catastrophic cyber-breaches that are taking place on the global stage, the massive breaches suffered by sophisticated international companies or state-sponsored cyber-terrorists stealing intelligence from government agencies such as the Reserve Bank of Australia. There is much talk of the looming threat, and while it is all very cutting-edge, what does it have to do with the daily life of ordinary Australian businesses?

What's going on?

Cyber threats are seen as one of the major challenges facing businesses today. A quick google search reveals a high level of interest in the possibility of future cyber events, as well as an increasing number of actual cyber-attacks.

The statistics are concerning, with companies such as web security experts Symantec citing that nearly one million new cyber threats were released online every day in 2014, with five out of six large companies globally targeted.[1]

The same report also found that 17% of all apps on Google's Android platform were actually malware in disguise.

There are also prophecies of an aircraft's controls being vulnerable to hacking by passengers using on-board WiFi if the system shares the same router with the plane, according to a US Government Accountability Office report released in April 2015.[2]

What about locally?

Interestingly, while the attacks on global companies such as Sony and Target retain the major headlines, the focus is shifting to the increasingly common but lower profile attacks on local Australian corporates, which are suffering an increased threat from spear-phishing attacks and ransomware.

In Australia, ransomware attacks using programmes such as CryptoLocker became more commonplace in 2014. While a major irritant for a home-user, ransomware could cause businesses to suffer actual losses through an inability to provide services.

Anecdotal evidence reveals a number of businesses locally have suffered attacks about which they are remaining tight-lipped, including one company that suspects it has been the victim of spyware and has had its operations and sensitive information secretly monitored by an unknown entity for some time. Queensland's resource operations are particularly vulnerable to such attacks given the highly-sensitive information they possess.

There have been a number of high profile attacks in Australia over the last few months, including:

1. In April 2015, Hobart Airport's website was hacked by ISIS supporters with messages of support for ISIS plastered over the website. The website was taken offline for several hours. The hackers gained access through domain host NetRegistry, in circumstances reminiscent of the Melbourne IT hacking in 2013 by the Syrian Electronic Army. No flights or the airport itself were affected.

   The costs to Hobart Airport would likely have been fairly minimal given that the website was not vital to its business, and no services were impacted. The loss would likely have been limited to re-setting the website.

2. In February 2015 Telstra, Optus and Vodafone confirmed that they had sold potentially millions of mobile phone SIM cards after it was revealed that US and British spy agencies stole encryption keys that secured personal information that was on the chips, including calls and texts. The SIM cards had been produced by Dutch company Gemalto.

   The losses associated with this hack are difficult to quantify and will take some time to ascertain. The telcos may incur significant costs in identifying the affected SIM cards if they have already been distributed. It is not clear how the telcos will approach customers who have bought a compromised SIM, but the customers' losses may be limited to the cost of the SIM. There is also, however, the possibility of privacy breaches arising out of the compromised personal information. There may be intermediary distributers also affected who could look to the telcos for their losses, who, in turn, would no doubt look to Gemalto to recover their costs and losses.

3. In December 2014, a notorious hacker known as Abdilo, who was actually a Queensland teenager, hacked into Aussie Travel Cover and executed one of the largest privacy breaches in Australian history when he released personal information of over 700,000 of Aussie Travel Cover's customers.

   The Information Commissioner is monitoring the fallout from the hack, and so it is not yet known if Aussie Travel Cover faces statutory liability for the breach. There are reports of its systems being down for a number of months over the busy Christmas period which, if true, would have caused business interruption losses. Apart from the reputational damage, it is not yet known in the public domain whether Aussie Travel Cover has any exposure to its customers or any financial institutions arising out of the misuse of the hacked information, which included credit card details.

Cyber risks need to be managed

Cyber risks can no longer be seen as something that exists only offshore. The risks will continue to grow as more and more companies seek to pursue innovation through the use of technology, as well as rely on electronic networks for their everyday functionality.

Companies should take a whole of business approach towards minimising cyber risks and the associated fall-out from a cyber event. Steps that businesses can undertake include:

1. Understanding the nature of the data they hold, and whether it is held on their behalf or is accessable by third parties;

2. Identifying the risks that this data faces from a cyber event;

3. Implementing effective risk strategies, procedures and protocols to protect the data;

4. Practising and preparing cyber event response and recovery procedures; and

5. Considering whether and how their present insurance coverage responds in the event of a data breach and whether obtaining specialised cyber risk insurance coverage is necessary.

[1] Symantec Security Response 2015 Internet Security Threat Report, Volume 20.
[2] United States Government Accountability Office, GAO-15-370, *Air Traffic Control: FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen*.

Authors

Katherine Hayes
Senior Associate

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

Greg Stirling
Associate

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