Hogan Lovells

Cyber security: A major issue for Australian business

Contents

FEBRUARY 2016

Want to know more?

If you would like further information or assistance, drop us an email or give us a call.

Tim Lester
Head of Corporate
Partner, Australia
T +61 8 6208 6551
+61 2 9093 3501
tim.lester@hoganlovells.com

Rebecca Cifelli
Senior Associate
Perth: +61 (0) 8 6189 8663
rebecca.cifelli@hoganlovells.com

Cyber security: A major issue for Australian business

Introduction and background

Cyber crime has become a major issue for Australian businesses. Although it is difficult to establish an accurate figure of how much cyber crime is costing Australian businesses, in a recent study the annual cost averaged across benchmarked organisations (thought to represent large Australian companies) was roughly $A4.9 million per year.[1] Business disruption appears to be the most expensive consequence of cyber crime, followed by information loss and revenue loss.[2]

Along with the private sector, the Australian government is also very concerned about the rise of cyber crime. Recently it has been reported that submarine builders in Germany, France and Japan bidding for a $20 billion contract to build a new Australian fleet have been subject to hacking attacks. The bidders were holding highly sensitive information about the Royal Australian Navy's technical requirements for its new-generation submarines. In response to the attacks the government indicated that it requires the companies it deals with to have the most thorough cyber security measures in place.[3]

More and more we are seeing businesses and government recognise the importance of implementing sound cyber security policies, both within their organisations and from their business partners.

Is your industry particularly vulnerable to a cyber attack?

The energy industry appears to be the most highly targeted with 29% of incidents responded to by CERT Australia occurring in this sector (CERT Australia is the point of contact in government for cyber security issues affecting major Australian businesses).[4] The banking and financial services and communications industries also reported a high number of incidents to CERT Australia.[5] Unsurprisingly, businesses in these industries that experience a high number of incidents also report experiencing substantially higher costs associated with cyber crime.[6]

Cyber security is a regulatory compliance issue in Australia

It makes good business sense for companies to ensure that they are adequately protected. However, for many businesses this is also a regulatory compliance issue. The Australian Securities and Investment Commission (**ASIC**) has advised, in its recent guidance note "Report 429: Cyber resilience: Health Check" issued in March 2015 (**the ASIC Guidance**), that it considers cyber resilience to be a high-risk area that will be considered in ASIC's surveillance programs of regulated entities. So it is important that companies understand the regulations and know what they need to do to comply. Depending on the severity of a breach, a failure to identify and manage cyber risk could result in fines, penalties, enforceable undertakings, licensing conditions or a licence suspension or cancellation. For directors or officers, a breach may result in disqualification.[7]

---

1 "2015 Cost of Cyber Crime Study: Australia", Ponemon Institute, September 2015.

2 "2015 Cost of Cyber Crime Study: Australia", Ponemon Institute, September 2015.

3 "Cyber torpedo alert: China, Russia hack submarine plans of bidders", *The Australian,* 9 November 2015; "Cyber security just can't hack it, says Peter Leahy", *The Australian,* 10 November 2015.

4 "Australian Cyber Security Centre 2015 Threat Report", 2015

5 "Australian Cyber Security Centre 2015 Threat Report", 2015

6 "2015 Cost of Cyber Crime Study: Australia", Ponemon Institute, September 2015.

7 *The ASIC Guidance*

The ASIC Guidance talks about "Cyber resilience", meaning the ability to prepare for, respond to and recover from a cyber attack. Resilience is more than just preventing or responding to an attack – it also takes into account the ability to operate during, and to adapt and recover, from such an event.

The regulatory requirements imposed on a company will depend on the nature of its business.

Of course, as noted above, some businesses are more exposed to cyber risks than others and ASIC has stated that they expect businesses to take a proportionate approach.

Directors

For directors, cyber risks may affect director's duties and annual director report disclosure requirements. For example, directors have duties to act with reasonable care and diligence.

Disclosure obligations

For companies with corporate disclosure requirements, cyber risks may need to be disclosed. This will depend on how exposed the business is to a cyber attack and if investors reasonably require information about cyber risks in order to make informed decisions. In particular, cyber risks may need to be addressed in a prospectus and/or annual report.

If a company suffers a cyber attack, it may need to disclose this as market-sensitive information.

Listed Entities

The Australian Securities Exchange's "Corporate Governance Principles and Recommendations" recommend that listed entities establish a sound risk management framework and periodically review the effectiveness of that framework. Cyber risks should be taken into account in this regard.

Entities regulated by the Privacy Act 1988 (Cth) (**Privacy Act**)

The Privacy Act regulates most Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses (collectively called 'APP entities').

APP entities must take reasonable steps to protect personal information they hold from misuse, interference and loss and from unauthorised access, use, modification or disclosure.

The Office of the Australian Information Commissioner (**OAIC**) recommends that, if there is a real risk of serious harm as a result of a data breach, the affected individuals and the OAIC be notified. We expect to see amendments to the Privacy Act making this a mandatory requirement in 2016. In December 2015 the Attorney-General's Department released an exposure draft of the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015*, which will, if passed, require entities subject to the Privacy Act to notify the OAIC and any affected individual of a "serious data breach".

A patchwork of regulations

In addition to the general regulations mentioned above, further regulations may apply depending on the nature of a particular business (for example, entities providing financial services will have additional obligations). In Australia there are no specific cyber security regulations that apply generally to Australian businesses. Rather, Australia has a patchwork of regulations that apply to different kinds of entities and create general obligations to manage risk and act with reasonable care. The ASIC Guidance has confirmed cyber security will be considered in the context of these general obligations. This means that it is important that businesses operating in Australia understand what regulations apply to them.

Progress in technology and increasing dependence on online systems mean that cyber security will continue to be a major issue for Australian businesses. Given the potential consequences of a cyber attack, it makes good business sense to be prepared with sound cyber security policies in place. It is also necessary given the regulatory obligations on Australian companies and their directors.

www.hoganlovells.com

Hogan Lovells has offices in:

Alicante
Amsterdam
Baltimore
Beijing
Brussels
Budapest*
Caracas
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jeddah*
Johannesburg
London
Los Angeles
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rio de Janeiro
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington DC
Zagreb*