Holding Redlich

Cybersecurity

Cybersecurity: How resilient are you?

Cyber risks: A significant cost to Australian business

The cost of malicious cyber activity, covering a broad range of actions including distributed denial of service attacks, phishing, data theft and ransomware attacks, to Australian businesses is now estimated to be more than $1 billion per annum. Such cyber activity may impact the ability of a company to carry on its business and also result in the theft or disclosure of confidential intellectual property and business information or personal information. This is a significant risk for all businesses, irrespective of size or industry sector. Accordingly, it is important for Australian businesses to take steps to build resilience into their business planning.

The impact on Australian businesses of cyber incidents

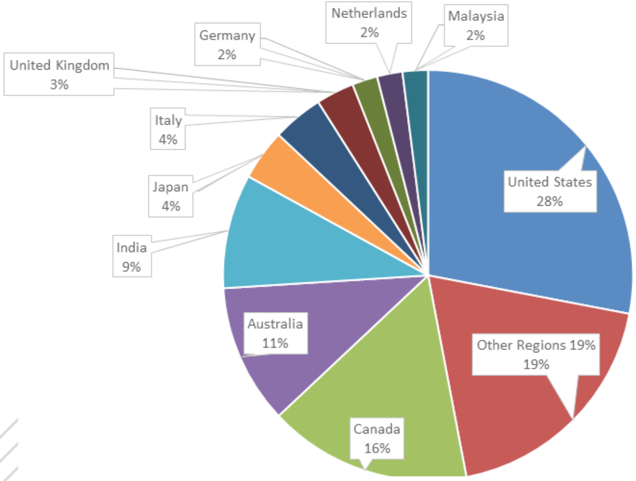
The potential impact of a cyber attack is demonstrated by the global Petya ransomware attack in late June 2017. Ransomware attacks lock users out of their IT systems and require payment of a ransom to provide access to data. Maersk, a global transport and logistics company, although not specifically targeted by the attack, was impacted. It shut down its IT systems for a period of time, with operations relying on a makeshift booking service constructed from scratch. Maersk has recently estimated that the cost of the attack was US$200 to US$300 million. The Petya attack impacted many businesses closer to home, with the Cadbury factory in Hobart shut down when computers stopped working and TNT Express also experiencing interruptions caused by the ransomware.

Although Petya and other similar global cyber attacks make headlines, there are many other cyber crimes that occur in Australia. Between July 2015 and June 2016 CERT Australia (the Australian Government's national Computer Emergency Response Team) responded on 14,804 cyber incidents affecting Australian businesses. This is likely to be only a small percentage of the incidents that occurred in Australia during that period, given reporting by businesses is voluntary.

And the risk is increasing

Data indicates that cybersecurity incidents are increasing. For example the following statistics shows Australian businesses are significantly impacted by ransomware infections.

Ransomware infections by region
January 2015 - April 2016



Source: Symantec, An ISTR Special Report: Ransomware and Business 2016

What is an appropriate cybersecurity strategy?

Combating cyber crime requires a holistic approach, encompassing people, processes and technology. Cybersecurity can no longer be treated as an IT issue. A properly formulated cybersecurity strategy, reflecting the nature of your business and risks, will help limit the chances of a successful cyber attack and also limit the negative consequences if one occurs.

There are three key phases for assessing your business's cyber risks and implementing an appropriate cybersecurity strategy that works for your business. These are:

- **Identify your critical data and IT systems**
  - This is a crucial first step.
  - Knowing what your critical data is, and where it is stored, as well as what your critical IT systems are, will assist in determining your risk appetite and the steps you need to take to protect your business.

- **Assess your current state of resilience**

  This requires an analysis of:

  - Responsibility and reporting lines for cybersecurity
  - Existing risk assessment and management plans
  - Resilience of IT systems
  - Existing policies and procedures
  - Incident management plans
  - Contractual arrangements
  - Legal compliance
  - Insurance

- **Implement an appropriate cybersecurity strategy**
  - Armed with the outcomes of the analysis above, a cybersecurity strategy would be formulated and implemented.
  - The strategy you need to be resilient will depend on the nature of your business and your risk appetite.

How can we assist you?

We can assist you in the following ways:

- **Scoping your initial review**
  - To assist in ensuring that all issues relevant to your business are considered.
- **Policies and procedures**
  - A cybersecurity strategy will include a number of technical and non-technical policies and procedures. We are able to assist with the non-technical policies.
  - Employee policies and training: Human error is often the cause of cyber incidents. Therefore increasing the cybersecurity awareness of your employees is very important.
  - Incident response plan: Even with the best of protections in place, a cyber breach may occur. An appropriate, tested incident response plan is critical. This would address allocation of responsibility; processes for confirming that a breach had occurred; categorisation of any breach; containment strategies; communications strategies and steps for dealing with customers; and processes for development of mitigation strategies to limit reoccurrence.
- **Governance and reporting**
  - Operational responsibility, and requirements for external review, should be clear.
  - Reporting lines should ensure that senior management and the board are appropriately informed and engaged.
- **Contractual framework**

  We are able to assist in reviewing and recommending changes to your:

  - ICT contracts: this includes contracts for general ICT services as well as contracts for the delivery of cybersecurity related services.
  - General commercial contracts: If you have significant online interaction (data and network sharing) with vendors, customers or other third parties.
  - Insurance policies, if these are necessary.
- **Legislative obligations**

  Your cybersecurity policy should ensure compliance with any applicable laws. This would include, for example, general director's duties under the *Corporations Act 2001* (Cth), the requirements of the *Privacy Act 1988* (Cth) and sector specific legislation where relevant.

About Holding Redlich

We are one of Australia's top 20 law firms. Using our law firm means that you receive commercial legal advice utilising the resources and expertise of more than 300 staff, including 122 lawyers and 47 partners, across offices in Melbourne, Sydney and Brisbane. We act for a broad range of Australia's largest public and private companies as well as Australian government entities, addressing some of their most complex and important commercial issues. We provide our clients with legal, commercial and strategic solutions founded on our legal and industry experience. And above all else, we understand that our job is to look after our clients and their best interests. Integrity and trust are at the core of our relationships with them.

Contact

Angela Flannery

Partner, Telecommunications, Media & Technology, Corporate & Commercial, Regulatory | Sydney

T +61 2 8083 0448
E angela.flannery@holdingredlich.com

Angela joined Holding Redlich in early 2017 as a partner in the firm's national Corporate and Commercial group. Angela has more than 20 years' experience as both a partner in private practice and in senior Commonwealth Government roles. She has particular expertise in the telecommunications, media and technology (TMT) areas, acting for clients in transactional and regulatory matters, including in telecommunications services and broader ICT contractual arrangements, regulatory reviews and cybersecurity audits and reviews. Angela has extensive knowledge of the regulatory framework governing the communications sector in Australia, including relating to telecommunications infrastructure, spectrum regulation, consumer regulation (including privacy) and the changing regulation in the media and content areas.

Disclaimer

The information in this publication is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, we do not guarantee that the information in this publication is accurate at the date it is received or that it will continue to be accurate in the future. We are not responsible for the information of any source to which a link is provided or reference is made and exclude all liability in connection with use of these sources.