MURFETT LEGAL
PROFESSIONALISM. UNDERSTANDING. RESULTS.

CORPORATE CYBER SECURITY & THE LAW: TRENDS TO LOOK OUT FOR IN 2020

As the world becomes ever more connected, cyber security has become a prominent key risk faced by many businesses. It has become increasingly important for organisations to stay ahead of the game by ensuring that its people and the business are as protected as possible.

The effectiveness of an organisation responding to any cyber security threat or incident will be largely dependent on the development of practices and procedures that should also be aimed at strengthening an organisation's cyber resilience.

As cyber security attackers are becoming more innovative, it is important to be aware of the trends so organisations can protect themselves accordingly. Murfett Legal have identified the following trends, and their legal implications, to look out for in 2020:

Cybersecurity and Directors' Duties

Company directors are no longer allowed to remain ignorant in regard to cyber security as it is a forefront threat faced by every business. Directors need to be proactive in their approach to cyber security by ensuring they have the necessary knowledge and understanding of cyber security threats to be able to establish and implement the necessary practices to protect the organisation. Without effective practices, including oversight and accountability, organisation's cyber security governance systems, policies and procedures can be rendered meaningless, leaving the enterprise vulnerable to attack and directors' can no longer claim ignorance to any allegations and claims made against them.

Data breaches can leave directors and officers of the companies attacked vulnerable to claims i.e. breaches of Privacy Law.

Courts have taken a broad approach in interpreting director's duties to include many aspects of cyber security, so to ensure directors comply with their duties, directors should, where

Level 2, 111 Wellington Street, East Perth WA 6004 • PO Box 6314, East Perth WA 6892
T: +61 8 9388 3100 • F: +61 8 9388 3105 • E: reception@murfett.com.au
ABN 74 120 362 825 • W: www.murfett.com.au

possible, acquire expert advice and have policies in place to deal with any potential breach and attacks.

The IoT (Internet of Things) Challenge

Simply put, the internet of things is connecting everyday “dumb items” i.e. heaters, lights, etc to a network connected to the internet allowing the items to ‘talk’ to one another. As with any device or network connected to the internet, IoTs are susceptible to the possibility of being hacked. Beyond the data breach that can follow as a result of hacking, there is also the issue of unauthorised surveillance.

The endless possibilities that are available with IoT proves to be a challenge to organisations, not only to keep up with the technology but to also ensure that as the organisation turns ‘smarter’ that process and procedures are in place to ensure that all data and personal information of personnel is also protected.

Shifting Attack Vectors & Cyber Hygiene Growth

An attack vector is the ‘path’ that hackers will utilise to gain access to a device or network to penetrate the system. The attack vector is not stagnant and the ongoing shift of attack vectors - from the networks to individual users – is requiring organisations to be vigilant in the management of cyber security. Largely in part by the awareness of many organisations recognising that their personnel (individual users) are often the weakest link.

As a result in the targeting of individuals, organisations need to be engaged in active and ongoing training of personnel to ensure that not only are they aware of cyber threats, but they also know how to deal with threats should they appear.

As personnel are considered to be the weakest link, it is crucial for organisations to have procedures in place to deal with both external cyber threats and internal cyber threats i.e. staff movements.

Courts can impose civil liabilities on an organisation in the event that organisation can be found to have been negligent, such as:

- an organisation failed to implement the necessary security and safeguards pursuant to regulations and statutes;
- an organisation failed to mitigate or remedy the damage of the breach; and
- an organisation fails to notify affected individuals and regulatory of breach notification pursuant to the relevant legislation (i.e. as of 23 February 2018, any breach considered to be ‘eligible data breach’ must be reported to the Office of the Australian Information Commissioner and any potentially affected individuals).

Cost and liability that may be imposed on an organisation, include, but are not limited to:

- claims and class actions by those affected by the breach, including shareholders;
- regulatory investigations and penalties; and

- increase of insurance premiums.

Cyber security is a very real threat to every organisation and it does not discriminate. Organisations can no longer be idle in their approach to cyber security. They must be proactive in their approach to combatting the threat. There are a number of legal practice areas that need to be addressed when dealing with cyber security (ie Privacy, Employment, Business structure etc). Murfett Legal can provide advice to your organisation in all of these areas and assist in the development of processes and procedures that your organisation needs to stay protected in the connected world of the 21st century.

Note: The above is a summary for general information purposes only. It is not intended to be comprehensive or constitute legal advice. You should seek formal legal or other professional advice in relation to your particular circumstances before relying on the content of this article.

For further information or assistance contact Murfett Legal on +61 8 9388 3100.

Author: Kelly Parker (Director: Business Advisory, Commercial & Insolvency)

Email: kelly.parker@murfett.com.au

Murfett Legal is a leading law firm in WA, providing services in litigation, corporate and commercial, employment and workplace relations, insolvency, debt collection, business restructuring, Wills & estates, property, leasing, settlements, liquor licensing and intellectual property.