October 2023

Commercial Insights

Cyber Security Awareness Month – Are you cyber aware?

October is Cyber Security Awareness Month (CSAM). CSAM is an annual reminder for Australians to stay safe online and protect their online information and assets.

The theme for CSAM 2023 is *'be cyber aware – don't compromise'*. CSAM is an opportunity for businesses to review their understanding of 'cyber security' as a concept while continuing to educate themselves on the cyber security landscape and current cyber security threats and best practices.

In this Commercial Insight, we explore what cyber security is and why it is important. We also review practical steps businesses can take to adopt the best practices of cyber security in this fast and ever-evolving online environment.

Is there an accepted definition of cyber security?

The phrase 'cyber security' is an elusive term that is becoming increasingly referenced but rarely defined.

While there is no one generally accepted definition, 'cyber security' can broadly be categorised as the organisation and collection of resources, technologies, processes and controls to protect cyber-enabled systems, networks, programs, devices and, ultimately, data and personal information from an attempt by cyber criminals to damage, destroy or infiltrate a computer network or system (also known as a cyber-attack).

Cyber security involves dynamic interaction between humans and systems and aims to broadly protect those persons or systems from intentional as well as incidental threats and cyber-attacks. With the ever-evolving nature of cyber threats, security measures need to be designed and regularly reviewed and updated.

Currently, most cyber security regulation in Australia is sector-based and subject to different regulatory frameworks. There is not currently one overarching set of regulatory requirements and compulsory standards that establishes cyber security obligations that businesses must comply with.

What is the impact of cybercrime?

Over the past year alone, Australian businesses have witnessed cyber-attacks and privacy breaches making headlines around the world. Latitude, Optus, Medibank and many other businesses have felt the

reputational and financial impact of cyber-attacks that have exposed the personal information of hundreds of thousands of Australians. Over the 2021-22 financial year, the Australian Cyber Security Centre (**ACSC**) reported receiving over 76,000 cybercrime reports, which equates to an increase of nearly 13% from the previous financial year and amounts to a report of cybercrime being received every seven minutes.

A lack of attention to cyber risks can result in financial costs by way of regulatory fines, damages, legal fees, lost revenue and business interruption, as well as significant non-financial costs such as reputational damage and loss of trust. Our ever-increasing reliance on technology only means that cyber risks are here to stay.

What practical steps should businesses take to address cyber security?

There are several steps you can take now to mitigate cyber security incidents, prepare your business to be cyber wise and significantly boost cyber security.

In promoting CSAM 2023, the ACSC is highlighting the following four simple steps:

1. **Update your devices regularly** – turn on automatic updates for all devices and software to ensure the latest security is in place at all times
2. **Turn on multi-factor authentication** – this adds another layer of protection to your accounts
3. **Back up your important files** – this helps to safeguard data from threats and avoid costly data recovery
4. **Use passphrases** (that is, a password that uses four or more random words) – and do not re-use passwords or passphrases as this could compromise accounts

In addition to taking the above steps, we also recommend:

1. **Reviewing your current cyber policies and positioning concerning remote working**.
   It is largely accepted post the COVID-19 pandemic that at least some form of remote working is here to stay. Therefore, businesses need to consider the cyber security risks that remote working may pose and adopt and update their cyber security policy to address the risks posed by:
   - unsecured wireless networks used to access the business' corporate network either in public or at home
   - employees using their own devices to work and ensuring that these devices adhere to cyber security protocols
   - personnel who are not aware of current cyber risks, increasing the likelihood of human error allowing a cyber-attack to infiltrate systems
2. **Your business keeps up to date with vulnerabilities and addresses any vulnerability promptly** - reducing the ability of cyber criminals to exploit known vulnerabilities

3. **Regularly testing your cyber security detection capability** - this includes incident response, business continuity and disaster recovery plans, and your risk register.

While the burden of safeguarding computer networks starts with senior management, ultimately all staff, no matter their position, are responsible for maintaining good cyber practices.

How we can help

Meridian Lawyers has experience working with clients to manage privacy and cyber security risk by ensuring that services, distribution, alliance, and other commercial arrangements support compliance with data protection laws and regulator requirements, with a particular emphasis on the insurance and health sectors. We also have experience in responding to data breaches and developing training materials.

This Insight was written by Special Counsel Hayley Bowman or Principal Mark Fitzgerald. For further information please contact Hayley or Mark.

Hayley Bowman

Special Counsel

+61 3 9810 6723

hbowman@meridianlawyers.com.au

Mark Fitzgerald

Principal

+61 3 9810 6767

mfitzgerald@meridianlawyers.com.au

Subscribe to receive our latest insights and updates on a regular basis.