Practice Area April 2020

Protecting Your Business from Cyber Threats During COVID-19

The COVID-19 global pandemic has seen a dramatic increase in employees working from home. While this has helped slow the rate at which COVID-19 is spreading through our community, it has presented an increase in cybersecurity issues. Businesses may therefore need to review and update their systems to ensure that they are protected against unwarranted cybersecurity threats. This includes reviewing current insurance cover.

Background

COVID-19 has potentially forever changed our daily lives, such as how we shop, socialise and work. It is not unusual to see exploitation occur during a crisis and the COVID-19 pandemic is no exception. An increase in malicious cyber activity across the internet due to the dramatic increase in employees working remotely continues to prove worrisome for businesses

Businesses should review their cyber risk profile and ensure they have appropriate risk management strategies in place to pre-emptively protect against cyber security threats. The harmful impacts of cyberterrorism are broad and can include loss of revenue, reputational damage and damage to equipment.

What are the Biggest Cyber Threats? Phishing Emails and Website Scams

Presently, Australian businesses are being targeted by coronavirus related scams and phishing emails, which the Australian Cyber Security Centre (ACSC) has advised will only increase in the coming months. These threats typically direct an individual towards a website that once opened either installs malicious software onto the individual's computer or steals their personal information. These websites often appear sophisticated, impersonating trusted entities such as the Australian Government or The World Health Organisation.

COVID-19 cyber scams have also been identified through the solicitation of personal information, including bank details, where individuals are invited to donate to a 'coronavirus charity fund'. Further scams include links to websites for 'the latest COVID-19 updates.

Often these cybersecurity scams will invite individuals to disclose personal information and ask for some type of identification, such as a driver's licence or passport, in order to validate an application or process.

Employees now working from home need to be even more cautious of malicious cyberattacks as remote working increases user vulnerability. This is due to:

- having to use electronic devices that do not have the same level of protection as their in-office computer;
- using unsecure wireless networks; and
- becoming increasingly reliant on video conferencing platforms, such as Zoom, to convey private information.

Due to these cyber threats, businesses need to consider having cyber insurance and risk management strategies in place.

This is in addition to how you acquire, store, manage and disseminate personal information.

Cyber Insurance

Cyber insurance helps to minimise the impacts of a cyberattack or data breach by providing mechanisms to control, contain and coordinate responses to cyber scams. It may help protect or minimise the aftereffects of a cyberattack by covering the cost of:

- repairing damage to computer systems;
- hiring legal and/or IT professionals to help recover data; and

- loss of income due to business disruptions.

It is therefore important for businesses to understand the terms and conditions of insurance arrangements to know if they are covered in the event of a cybersecurity breach, and to review their cover.

It is crucial that businesses understand and appreciate the severity of a cyberattack. One of the biggest differentiating factors is the lack of physical or geographical containment of a cyber breach, meaning the attack can occur at anytime from anywhere in the world, and can thus be untraceable.

While businesses may recoup financial losses incurred from a cyberattack, if the loss is measurable, any damage to reputation through leaked information for example, is not easily compensable by an insurer.

Indemnity insurance for a cyberattack should therefore be viewed as the last level of protection.

Risk Management

Businesses need to consider employing pre-emptive mitigation strategies to protect against COVID-19 scams, such as, but not limited to:

- Not opening any attachments or any links on unsolicited emails or messages;
- Not responding to unsolicited messages or calls that ask for personal or financial details;
- Checking the sender names, email addresses, phone numbers, and attachment names before actioning the correspondence received to ensure its validity;
- Performing a simple google search of sender addresses or business names to ensure details are correct; and
- Calling organisations using their official number listed on their website, rather than different phone numbers listed in an unsolicited email.

Importantly, businesses must also ensure their system software is up to date with the most recent security patches and consider implementing multi-factor authentication for remote access systems.

Staff should also be informed and educated about good cyber security practices, particularly in relation to common threats as described above. This also extends to making sure employees have physical security measures in place to minimise the risk that information is accessed, used, modified or removed from an individual's remote working location without authorisation.

Effective implementation of these strategies will assist businesses to be digitally safe while being socially distant.

Employee Cyberhealth

While it is important for businesses to ensure that their cybersecurity system is up to date and healthy, consideration must also be given to employee mental health.

Employees working remotely may be experiencing increased levels of stress related to their home environment. Such stressors can be related to caring for children, increased relationship tension, alongside the new challenges of working outside the office.

Increased levels of stress can place employees in vulnerable positions when it comes to cybersecurity threats. It is therefore in the best interests of the business to connect and 'check-in' with their employees while they are working remotely to try to reduce any unwarranted stress.

Safe Work Australia has published several tips for businesses to how to manage the stress of their employees while working from home. Such tips include regularly communicating with staff, providing points of contact to discuss any concerns that may arise and proactively supporting at risk workers.

Further Information

Businesses should stay informed and up to date with any further guidance released by the Government. If you are concerned about your privacy obligations during COVID19, please contact us.

Please note: this information is current as of 15 April 2020. The speed with which COVID-19 is spreading and the varied responses both internally within Australia and externally change daily. It is important that you regularly keep up to date with all relevant information and be prepared to respond as the landscape in which the virus is moving changes. Keep up to date on COVID-19 legal issues through our website here.

Contact details

Ralph Bönig *Special Counsel*
Ralph.bonig@finlaysons.com.au

Lan Lam *Partner*
Lan.Lam@finlaysons.com.au

Adam Hamilton *Law Clerk*
Adam.Hamilton@finlaysons.com.au