BUDDLEFINDLAY

Cyber security and COVID-19 – how to stay safe online

Allan Yeoman, Amy Ryburn, Philip Wood, Renee Stiles, Alex Chapman, Damien Steel-Baker, Keri Johansson

30 March 2020

New Zealand businesses and employees have been readjusting to a new way of working over the past week following the Government's increased response to tackle the spread of COVID-19 in New Zealand. The adoption of working from home practices at an unprecedented speed has introduced new challenges and cyber security risks for businesses and employees seeking to adjust to a new type of working day.

While we have previously commented (here and here) on how businesses can manage a decentralised home-based work force from an employment perspective, it is also important that businesses adopt (to the extent that they have not already done so) and maintain robust cyber security practices to manage this new transition over the coming weeks. In light of the COVID-19 specific cyber security guidance issued by the World Health Organisation, the New Zealand National Cyber Security Centre and CERT NZ, we have summarised below three key issues for New Zealand businesses to consider in managing the cyber security risks associated with employees working remotely.

Avoid phishing spam emails and text messages claiming to have updated COVID-19 information

There has unfortunately been an increase in unsolicited emails and text messages which contain fictitious safety measures and which are designed to take advantage of the uncertainty surrounding COVID-19. Businesses, to the extent that they have not already done so, should:

- Ensure that employees are educated about the emerging types of phishing scams (both generally and those related to COVID-19 in particular)
- Advise employees not to open any suspicious correspondence or malicious links
- Ensure that there are internal processes and policies in place for notifying internal technology support personnel on any suspicious correspondence.

Ensure employees are resourced appropriately

As we have commented before, it is important to ensure that staff are resourced appropriately in terms of hardware, software and connectivity options. In particular, there is a risk that in working from home, employees may connect to public and unsecured Wi-Fi connections, which may be more susceptible to security breaches. Businesses should ensure that their internal technology policies prohibit employees connecting to unsecured public Wi-Fi and that employees are aware of those policies. If employees are unable to connect to a secure Wi-Fi network, businesses may want to consider what alternative arrangements can be put in place (eg portable modems). Many employees will also be rushing to download or sign up to video conferencing and other software tools. While most commonly-used applications are reliable and reputable, it may be worth steering employees in the direction of applications and services that meet the organisation's privacy and security requirements (and circulating a 'blacklist' of ones to avoid).

Maintain confidentiality of sensitive documents and devices

Businesses may also wish to consider whether employees should be discouraged from using their personal devices to download and access business related information, unless they are confident that appropriate security protections have been applied to those personal devices. If employees are permitted to use their own personal devices, businesses should consider the extent to which monitoring tools will be applied to those devices and whether any updates are required to internal technology policies to reflect that monitoring.

Businesses may also want to remind employees that physical security is just as important as digital security when working remotely and encourage employees to keep hardcopy business sensitive documents securely stored at home and to ensure that their devices are password protected.

Auckland

PwC Tower
188 Quay Street
Auckland 1010

PO Box 1433
Auckland 1140
New Zealand

P: +64 9 358 2555
F: +64 9 358 2055

Wellington

Aon Centre
1 Willis Street
Wellington 6011

PO Box 2694
Wellington 6140
New Zealand

P: +64 4 499 4242
F: +64 4 499 4141

Christchurch

83 Victoria Street
Christchurch 8013

PO Box 322
Christchurch 8140
New Zealand

P: +64 3 379 1747
F: +64 3 379 5659