DWFoxTucker Lawyers

Alert

INTELLECTUAL PROPERTY

COVID-19: IT Security and Working From Home

By Sandy Donaldson, Amy Bishop & Victoria Malcolm

Health and economic concerns have been priority issues during the early stage of the COVID-19 pandemic. However, as we settle in to a working from home (**WFH**) routine, IT and cybersecurity should also be prioritised and carefully considered by employers and employees.

Employers to whom the *Privacy Act 1988* (Cth) applies will likely already have in place mechanisms for keeping data containing personal information secure in compliance with their obligations under the Australian Privacy Principles and their obligations in relation to Notifiable Data Breaches. These obligations are ongoing and will continue to apply as employees work from home but with new and altered risks.

Even for employers to whom the *Privacy Act 1988* (Cth) reporting obligations do not apply, there are IT security risks which should be identified and addressed as they relate to recent WFH changes. In fact, in some circumstances, smaller entities may be more vulnerable to risks as resources may be limited and IT security may not have previously been addressed.

The WFH model will usually result in a significant increase in the number of devices accessing a network and additional risks of a data breach. IT security issues which were once only confined to a single workplace may now be extended to each individual employee's home. Cybersecurity and data breach policies and risk management plans should be updated, new risks identified, and mitigation strategies put in place.

We have put together a practical guide on IT matters for employers to consider in respect of WFH arrangements:

– Devices

When employees use personal devices (i.e. desktop computers, laptops and tablets) to access commercially sensitive business data and a customer's personal information, it increases the risk of this data being exposed to a severe threat.

This risk can be reduced by, where possible, having employees access the organisation's data and systems only through remote access VPN's.

Employers should enforce a policy that directs employees to only use work email accounts, not personal accounts, for all work-related emails. They should also be discouraged from saving any work to their personal devices and, should they need to do so, be required to delete it as soon as it is no longer needed.

All devices being used for work purposes, as well as VPNs and firewalls, should maintain the most recent updates and security patches. Finally, it is essential to ensure that all employees' devices are equipped with protection through the use of antivirus software.

– Wi-Fi

Use of Wi-Fi from home or out of the workplace poses risks, particularly in relation to the use of unsecured Wi-Fi networks. Wi-Fi should only be accessed on secured networks, and employees should be required to configure their devices to ensure that they are not automatically connecting

continued overleaf...

to unsecured open Wi-Fi networks. Wi-Fi utilised during any WFH arrangements should be checked to ensure that networks are properly secured.

– Password protection

As always, security should be maintained through the use of proper password protocol. Employees need to have strong passwords for their devices and VPN connections, such as passwords comprising at least ten characters made up of upper and lower case letters, numbers and symbols. Where possible, two-factor authentication should be utilised for remote access systems and resources (including cloud services).

– Communications platforms

The way we are communicating and staying connected has changed, and collaborations are being conducted on various platforms, such as Microsoft Teams, Zoom, Houseparty and WhatsApp. Whether a platform is 'safe' to use depends on the features it provides and the purpose for which it is being used. Some platforms provide security functions such as end-to-end encryption and other security features to prevent interception such as cryptographic protocols like TLS and SSL. Decisions about whether a particular platform is suitable for use by an organisation should be made in consultation with an IT professional based on the organisations' needs and the intended use of the platform.

– Scams and fraud

Targeted malicious activities are not something new for organisations to deal with; however, employers need to ensure employees continue to be provided with adequate training to remain alert to such activities. Scams can be highly sophisticated, and employees should be reminded to be wary of suspicious attachments and avoid clicking on links from unknown sources. Emails containing bank account details should not be trusted and should be verified by phone or other means to ensure that emails have not been intercepted and a scammer's bank account details inserted.

There have already been a number of scams circulating in relation to COVID-19 including those which utilise Government impersonations and online shopping scams. For examples of scams relating to COVID-19, please refer to the Scamwatch website[1].

– Data breach

Where organisations are required to investigate and report possible data breaches, employees setup to WFH must advise employers as to any irregular or unusual activities which may amount to potential data breaches. As discussed above, obligations concerning the Notifiable Data Breaches Scheme are ongoing, and employers are going to be heavily reliant on employees reporting any suspicious activity or potential breaches to them for further investigation.

It is recommended that any Data Breach Response Plan be reviewed to ensure that it remains a suitable plan in the event of a data breach and can be implemented in the current environment. Proper investigations of possible data breaches must be undertaken and completed within 30 days.

– Updating operating systems

Operating systems should be reviewed and updated as necessary. Use of operating systems which have not been updated carry with them certain vulnerabilities. Protection from such risks may be mitigated by ensuring operating systems are kept updated and ensuring automatic updates are turned on.

As employees may not operate on the same operating systems from home, each employee's home set up should be considered, and updates rolled out as necessary.

– Transferring files and data

Consider how information is to be transferred between the workplace and home. Where possible information should be transferred through a secure means, such as through a properly protected cloud system, and should be protected through end-to-end encryption.

1 https://www.scamwatch.gov.au/types-of-scams/current-covid-19-coronavirus-scams

continued overleaf...

Where possible, data should not be transferred on portable devices such as USB's or portable hard drives as these are easily lost. If USB's or similar devices must be used, then these should be erased immediately after the data has been transferred.

– Physical documents

Some employees may need to have documents at home, which contain personal, confidential or sensitive information. These need to be kept secure while in the home, such as in a locked filing cabinet. Employees also need to be told not to simply dispose of such documents in home rubbish bins but shredded or later returned to the employer to be disposed of in the same manner they would ordinarily be.

– Cameras

Turning off webcams after these have been used in online meetings is highly recommended. There have been many instances of hackers spying on people through cameras that are left on.

– Remote Deletion

Employees should be required to notify their employer immediately if a phone or other device of the employee is lost or stolen. Android and iPhones have the capability for remote erasure and deletion of data, and this may be possible if this is set up on PCs.

The above guide is by no means an exhaustive list of IT security considerations which may be relevant, and every organisation will have a unique set of circumstances that require specific needs. Discussion of specific requirements with an IT professional could address some of the issues raised. In addition, all relevant and necessary considerations should be expressed in an IT Policy, whether as an amendment to an existing policy or a new COVID-19 specific policy. It is essential to circulate any new or changed policy to employees and ensure they are aware of and actively implementing the matters addressed in the policy. It is best practice to have employees agree to abide by any policies, and well-drafted employment contracts are likely to already provide for this.

If you have any concerns or queries in relation to your IT and cybersecurity risks or obligations due to staff now having to work from home, please contact one of our experts.

MORE INFO
Sandy Donaldson Director
p: +61 8 **8124 1954**
sandy.donaldson@dwfoxtucker.com.au

MORE INFO
Amy Bishop Senior Associate
p: +61 8 **8124 1827**
amy.bishop@dwfoxtucker.com.au

DW Fox Tucker Lawyers
L14, 100 King William Street, Adelaide, SA 5000
p: +61 8 **8124 1811** e: info@dwfoxtucker.com.au **dwfoxtucker.com.au**

COMMERCIAL | CORPORATE | DISPUTES | FAMILY | INSOLVENCY | TAX | HOSPITALITY | IP | PROPERTY | ENERGY | RESOURCES
EMPLOYMENT | WORKERS COMPENSATION | SELF INSURANCE | RISK MANAGEMENT | INSURANCE | WILLS | ESTATE PLANNING