COVID-19: (AUSTRALIA) FORGOTTEN ISSUES: WHAT BUSINESS CONTINUITY PLANNING IN THE COVID-19 ERA ISN'T CONTEMPLATING

Date: 30 March 2020

By: Cameron Abbott, Warwick Andersen, Max Evans

**This information is accurate as of 7.00 pm Monday 30 March 2020 and is subject to change as this situation evolves.*

As the world grinds to a halt following the dispersion of COVID-19 and businesses around the globe experience a significant downturn, more and more businesses are turning to their Business Continuity Plan (BCP) to mitigate the potential impacts of this worldwide emergency on business sustainability. However, a key aspect of BCPs are that they encapsulate the full scale of collateral issues that may arise from such an emergency.

From a technology perspective, BCPs need to consider access. This issue is twofold: having access to premises in which businesses operate in order to correct system defects and system outages, as well as access to external premises that provide technology services such as data storage or data security services.

In the former scenario, the increasing amount of restrictions placed by Landlords on access to business premises may require businesses to obtain the consent of their Landlord prior to accessing a premises or any locations where, for example, equipment or ducting for cabling is located. This may mean that lead times to fix outstanding issues increase from minutes to hours or even days. Therefore, businesses need to identify their access process, and have procedures in place to swiftly obtain any consents and rectify any future issues. Businesses also need to include in their BCPs alternative solutions should requests for consent to access be delayed or rejected, to ensure business processes continue to function.

In the latter scenario, external service providers such as data centres may impose restrictions or even bans on access. This is already occurring elsewhere in the world, and will surely be adopted by those same international operators in Australia as the virus impact expands. Data centres are high risk environments for a virus (and for a change we are not talking about a computer based virus!). Warm air with filters that were mostly designed to filter external air coming in (not internal air circulating), are encouraging environments for COVID-19. It is not surprising therefore that data centre operators conclude that the best approach is preventing entry.

This could impact significantly on a business if infrastructure fails and needs to be fixed or even re-booted. We are seeing in other countries these operators excluding access and requiring any activities to be dealt with by their staff on a first come first served basis regardless of urgency/severity. Failover capability becomes increasingly important when you cannot gain access onsite to conduct remediation.

Therefore, our message is simple. In this unprecedented era, think deeper about your BCPs. In particular, the impact of access restrictions and prohibitions, as you may not be able to obtain regular access to do what you normally do to fix your technology systems, with potentially dire consequences on business sustainability.

KEY CONTACTS

CAMERON ABBOTT
PARTNER

MELBOURNE
+61.3.9640.4261
CAMERON.ABBOTT@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.