Cyber risk during Covid-19 outbreak

By Rosalind Lake and Priyanka Naidoo

19 Mar 2020

A common response by businesses to the spread of the coronavirus (Covid-19) has been to implement measures that require social distancing and remote working. To ensure business continuity, some of these measures rely on the availability of technology like VPN access, as well as the use of online platforms to hold team meetings, client calls, vendor engagement, and even mediation proceedings.

© Jakub Jirsak – 123RF.com

On 15 March 2020, it was reported that the US Department of Health and Human Services suffered a hack, which was apparently aimed at slowing down HHS computer systems during its response to the spread of Covid-19. Even though HHS reported that there was no actual exfiltration of data, it was subsequently discovered that false information was being circulated about a national quarantine. The false information campaigns were apparently linked to the hack.

Businesses are reminded to ensure that their computer systems are resistant to cyber threats and that employees' cyber hygiene is prioritised. This is especially a risk for those businesses that are not used to remote working and relying on such technology, and whose inexperience may lead to them easily falling victim to a phishing attack.

Businesses should also ensure that they have appropriate measures in place to respond to a data breach should one occur. This is especially relevant to those businesses whose employees are working remotely. It can be challenging for forensic experts to implement mitigation steps when compromised devices and work stations may be off-site. Businesses are encouraged to speak to their IT teams and forensic experts to determine their response capabilities.

The existence of Covid-19 and the extraordinary governmental measures do not automatically excuse parties from taking

measures to protect personal and confidential information. Even though POPIA is not yet in force (and therefore there is no need to account formally to the Information Regulator till it is), companies have common law and possibly contractual obligations to secure information and must continue to protect their reputation in these challenging times. This is especially so when access to personal health information could expose individuals to significant harm. Companies must include cyber risk as part of their Covid-19 response plan and make sure that remote-working employees know what to do in a cyber-emergency.

ABOUT THE AUTHOR

Rosalind Lake is a Director and Priyanka Naidoo, an Associate Designate, at Norton Rose Fulbright.