The COVID-19 virus has forced substantially increased numbers of employees to work from home, potentially for an extended period of time. Against an already cluttered landscape of other business-critical issues they have to deal with, businesses also need to be mindful of the increased risk to cyber, and other types of data security, that this presents. This risk is amplified where employees are required to use personal devices to access business information, due to the limited supply of work devices.

Recent reports suggest that hackers and other malicious actors are already taking advantage of potentially weakened technology systems and the increased opportunities for cyber-crime, making it all the more important to try to maintain both technical and organizational measures to protect data, during the crisis.

Employers are advised to remind employees that whilst accessing work-related information and networks from home, they must continue to comply with all relevant company policies and procedures, particularly relating to confidentiality and data security. It may be useful to highlight certain measures that will be particularly important at this time, such as:

- Ensuring that mobile devices (such as mobiles, laptops and iPads) that are used to access business information are password protected in line with the company’s IT security policy and are not left unattended at any time;
• Reminding employees to stay vigilant against phishing attempts, including not to open any emails that appear to be suspicious and instead to forward them straight to their IT Support department for review and not to click on links and/or enter login/password details unless they are 100% certain of their origin;
• Preventing unauthorized access to work-related information and systems, including by family and friends that employees may be self-isolating with;
• Warning employees not to connect to internet sites on devices used to access company information, unless they are sure that they are secure;
• Not to use shared or public computers to access company information; and
• In the event that an employee becomes aware of, or suspects that there has been any unauthorized access to company information, to immediately contact IT support or other contact with responsibility for managing data breaches within the organization. It’s worth making the point that prompt notification of any suspicious activity, provides the business with the greatest opportunity to protect data by stopping unauthorized access (such as by remotely wiping the device) and thereby preventing or limiting any resulting damage.

© Copyright 2020 Squire Patton Boggs (US) LLP