BCLP. Client Intelligent

Insights

LAPTOP SECURITY IN THE US: WORKING FROM HOME CYBERSECURITY BASICS

Apr 06, 2020

SUMMARY

As the Covid-19 Pandemic forces more employees than ever before to work from home ("WFH"), businesses face new and different data privacy and security risks. This change is not lost on U.S. regulators, but it does not mean that businesses will get a pass on data privacy and security issues potentially caused by the shift in working conditions. In an effort to help businesses navigate these new circumstances, BCLP has prepared a series of articles on addressing data privacy and security issues in a WFH environment.

With employees carrying their laptops home from work, now is a good time to remind them and your IT staff of some common sense steps to keep their laptops safe and secure while out of the office.

- **Passwords**. Make sure each laptop is secured with a user account that requires a strong password to access it. Additionally, make sure the laptop's user account only has limited privileges and that an IT-only administrator account is also secured with a complex password.
- **Locked**. Laptops have a habit of walking away if not securely locked down or up. A best practice for any laptop is to secure it with a sturdy laptop lock to the desk it is kept on. Failing that, locking a laptop in a sturdy desk drawer or other secured cabinet also works. If no lock is available, hiding the laptop provides a lesser measure of protection, although it is less secure than locking the device down.
- **Encryption**. Depending on the device, your laptops may support full disk encryption. If it is available, full disk encryption provides powerful, best in class protection for data stored on laptops, provided that the password securing the device is a strong, complex password.
- **Location tracking**. Some laptops and operating systems support location tracking in case the device is lost or stolen. Notify employees of this capability and its use, as this tool can provide

a measure of comfort in times where more systems are out of the building than might normally be expected.

The Federal Trade Commission ("FTC") in its advice to businesses on WFH security noted that employees should not leave their laptops unattended in public places. For the time being, caution your employees against going to public places to do work. If they must travel, remind your employees to keep a close eye on their laptops at all times.

This article is part of a multi-part series published by BCLP to help companies understand and cope with data security and privacy issues impacted by the Covid-19 Pandemic. You can find more information on specific data privacy and security issues in BCLP's California Consumer Privacy Act Practical Guide.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Oran Gelb

London

oran.gelb@bclplaw.com
+44 (0) 20 3400 4168