BCLP. Client Intelligent

Insights

GENERAL TIPS FROM THE FTC IN THE US: WORKING FROM HOME CYBERSECURITY BASICS

Apr 09, 2020

SUMMARY

With the Covid-19 Pandemic forcing 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.

As part of its initial guidance[1] to businesses on working from home during the Covid-19 Pandemic, the Federal Trade Commission ("FTC") advised businesses to start with cybersecurity basics[2] when assisting employees in setting up their WFH operations. That advice included:

- **Updating software.** The FTC mentioned updating browsers, apps, and your computer's operating system. The FTC also suggested making updates automatic.
- **Securing files.** This means backing up important files on external hard drives and cloud storage systems and securing any paper files at home.
- **Requiring passwords.** The FTC suggests requiring passwords to log into laptops, phones, and tablets and making sure not to leave those devices unattended in public places.
- **Encrypting devices.** To the FTC, this means encrypting any device with sensitive personal information such as laptops, removable storage, removable media (DVDs), backup tapes, and cloud storage.
- **Using multifactor authentication.** The FTC would prefer that businesses use multifactor authentication to access any systems that store sensitive information. This means requiring

something more than a username and password to access the system, *g.*, a second factor, like a token or push notification.

In practice, some of this advice is difficult to implement under the best of circumstances (setting up encryption on devices is, typically, a major project for even a small business).

To the extent that your company can implement the FTC's guidance with a reasonable amount of effort, it should; the advice is good and will help to keep your data protected. However, to the extent that your company does not have the resources, be it money, IT employees' time, etc., you can document your company's assessment of the advice, note the places where resource constraints prevent you from taking the FTC's advice, and then document a compensating control that you might be able to implement in its place.

For example, perhaps your employees handle highly sensitive information on a regular basis. While encryption is a very good idea for their devices, your company has not yet implemented full disk laptop encryption. In this instance, try to find another sensible process to help secure the sensitive information. For example, create a policy where employees must securely save their sensitive files, such as in an encrypted cloud solution, at the end of each day and then securely delete the files from their laptop.

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.

1. www.consumer.ftc.gov/blog/2020/03/online-security-tips-working-home

2. www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/basics

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Oran Gelb

London

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