Cyber Security Best Practices: Post COVID Remote Work

COVID 19: Answers to Business Challenges, News, Privacy, Technology and Data Security July 17, 2020

J. Andrew Salemme asalemme@tuckerlaw.com (412) 594-3952

In the wake of the COVID-19 pandemic many businesses and employers have begun to rely on their employees working primarily or even exclusively remotely. As a result, many employees are utilizing either their own smartphones, tablets or laptops and other mobile devices or those provided by their employer to conduct business. While working remotely offers great flexibility and the ability to continue operating during the COVID-19 pandemic in a physically safe manner, it also poses additional data security risks. Employers and employees must be ever vigilant against cyberattacks, including phishing, malware and other attempts by cybercriminals to exploit the often rapid transition to a remote workforce. For those businesses that are new to remote work or even for those that consider remote work "old hat" it is a good time to either create, review or revamp security guidelines and policies governing remote work.

For example:

- Employees working remotely should avoid the use of unsecured public Wi-Fi;
- Employers also may wish to establish a Virtual Private Network (VPN) and require employees to use that network when working remotely and establish what is called a multi-factor authentication. VPNs allow employees to connect to the employer's internal network and provide an extra-level of protection–but there are varying qualities of VPNs and businesses should be mindful of selecting one that suits its needs;
- Employers should strongly consider providing guidance to their employees regarding saving documents to a personal device, the use of USB devices to save information, and the sending of documents to a personal e-mail, all of which may not be secure;
- Employees should also have up-to-date firewalls and anti-virus/malware software on all of their devices.

All of these areas are methods of securing data that can be outlined in a data security policy. Policies establishing protocols for how employees can use their own devices or employer provided devices and that inform employees of the importance of data security is a relatively simple but important first step in protecting customer/client data. Such policies can not only educate employees but help to ensure the security of customer/client data.

For current information on data security, visit our COVID-19: Answer to Business Challenges and Privacy, Technology and Data Security Blogs.

For additonal information contact Andrew Salemme.