BURR ALERT

# COVID-19 Cybersecurity Considerations for a Remote Workforce

By Elizabeth B. Shirley & Brooke R. Watson April 2020

Only a few days ago, President Trump extended social distancing guidelines to April 30, 2020. In addition to the measures taken by the federal government, the majority of states have implemented shelter-in-place orders lasting until late April, and even more have enacted orders requiring all non-essential businesses to remain closed on a similar timeframe. While most current guidance lasts only through late April and early May, there appears to be no guarantee that these orders and social distancing guidelines may be lifted at that point.

While shelter-in-place orders typically only limit the activities of non-essential businesses, even essential businesses have permitted employees whose jobs do not require presence at the business to work remotely. There is no doubt that COVID-19 has changed the nature of how Americans work for the foreseeable future, and the presence of a remote workforce will likely continue even after COVID-19 is a distant memory. Therefore, it is important for employers to keep in mind that the apprehension due to COVID-19 and the remote workforce it has implemented may bring a heightened likelihood of cyberthreats. In order to protect your business from cybercriminals hoping to capitalize on the effects of COVID-19, employees and employers should do the following:

- **Encourage employees to think critically before they act.** Cybercriminals are highly skilled and use psychology to attempt to capitalize on individuals' weaknesses in a time of fear. This highly turbulent time is no different, and cybercriminals try to use the serious nature of the situation to their advantage. By thinking critically before clicking a link, opening a suspicious email, visiting a questionable website, or divulging valuable business information in a phone call, your employees can lessen the probability of subjecting your business to a cyberattack.

- **Only visit trusted websites on work computers or while remotely connected.** Whether or not during the COVID-19 pandemic, employees using devices issued by their employer or using remote connectivity services to login to their employer's network should only visit trusted websites. Employers should ensure that they have up-to-date policies and security measures regarding use of employer-issued computers, employees' internet use, and employees' use of personal (as opposed to work-issued) devices. Employers should closely monitor employees' use of these tools to ensure compliance. Employers should require the same security measures on personal devices as are required for work-issued devices.

- **Keep your username and password confidential.** Login credentials should always remain confidential since they are often a target of hackers. However, during this time, cybercriminals may fraudulently assert that they need your login credentials to allow an employer to setup new software or assist with teleworking issues. Never share your login credentials with anyone.

Employers that have not started using two-factor authentication for remote access should do so as soon as possible.

- **In cybersecurity, your gut can be an essential asset.** When you receive a potentially fraudulent email or phone call, and you are unsure of whether it is legitimate, *always* listen to your gut. In the world of cybersecurity, if it "feels" devious, then it likely is devious.

If you experience a cyberattack, or if you have questions about internet-use policies, employer-issued device policies, or implementing two-factor authentication for remote connectivity, please do not hesitate to contact Burr's Cybersecurity Team.

**To discuss further, please contact:**

Elizabeth B. Shirley in Birmingham at bshirley@burr.com or 205-458-5186,

Brooke R. Watson in Birmingham at bwatson@burr.com or 205-458-5165,

or the Chair of our Cybersecurity group, India E. Vincent in Birmingham at ivincent@burr.com or 205-458-5284.