COVID-19 and Cybersecurity for Remote Work

Date: 04/07/20

COVID-19 has forced businesses to undertake an unprecedented shift towards remote work. With social distancing and quarantines becoming the new norm, cyber criminals already are taking advantage of these sudden and unexpected changes in behavior, and authorities have reported a predictable spike in COVID-19-related cyberattacks, particularly phishing emails, robocalls, and similar scams.

As companies shift to working remotely, cyber criminals actively are refining their attacks. In this new environment, potential victims will face new and unexpected difficulties separating legitimate business requests from illegitimate scammers' tricks. For example, the increased use of personal devices and extensive remote access to company information systems heighten the vulnerability to hackers who may slip in a last-minute change to payment instructions that is purportedly explained by ongoing events and appears entirely authentic. The resulting losses can be as large as the amount of a corporation's largest wire transaction. To address these new risks and maintain business continuity, companies must reassess and reevaluate their cybersecurity operations. We outline below a variety of factors for companies to consider when doing so.

Attorney

- David R. Owen