msk

careful with the remote

Cybersecurity Concerns with Remote Work
Susan Kohn Ross and Timothy Carter
MSK Client Alert

March 23, 2020

While likely not the first topic that comes to mind amidst a global pandemic, organizations and businesses that now find themselves entirely (or almost entirely) remote would be remiss not to consider the potential data and cybersecurity issues raised by this sudden and unexpected shift to remote work. For much of the country, COVID-19 has resulted in an abrupt shift in the way we work. Even for those businesses that maintained robust work-from-home policies and systems, this shift presents a learning curve. The more traditional data and cybersecurity concerns ever-present in normal business operations are compounded by the difficulties presented by an extensive remote workforce. Preoccupied remote workers can be more susceptible to online threats such as phishing emails or malware and ransomware, thereby "opening the door" and providing unauthorized access to bad actors. The other, often lesser considered concern is accidental disclosure of confidential business information.

While some professions undoubtedly deal with confidential materials more frequently than others, most businesses maintain sensitive company information, and with a significant chunk of their workforce now unexpectedly remote, businesses will want to be mindful of the complications remote work poses for maintaining confidential information, whether that data consists of employee or customer personal information, trade secrets, or tax and other financial information.

View Full Alert

attorneys

Susan Kohn Ross

practice areas

cybersecurity and privacy

regulatory