BLANKROME

Cybersecurity & Data Privacy

MARCH 2020 • NO. 3

Coronavirus Update: Practical Considerations for Remote Working Arrangements

In recent weeks, the coronavirus ("COVID-19") has swept across the United States, with documented cases increasing exponentially on a daily basis. As drastic measures continue to be taken both abroad and here at home to slow the spread of the virus, companies now face the stark reality that remote working arrangements for employees may no longer be just an elective, precautionary measure, but instead may soon become an absolute necessity. Importantly, remote working creates a number of unique, sizeable cybersecurity and data security challenges that are not commonly seen with traditional work arrangements. As such, companies must be prepared to quickly implement measures and protocols to ensure the security of their networks, systems, and sensitive data in the event they elect, or are required, to put in place remote working programs in response to the coronavirus epidemic.

THE HEIGHTENED SECURITY THREAT POSED BY REMOTE WORKING ARRANGEMENTS

Some of the world's largest companies, such as Apple, Twitter, Facebook, and Procter & Gamble, are encouraging employees to work from home as coronavirus cases rise across the country, and many other businesses are considering following suit. While remote working can aid in shielding employees from contracting the coronavirus, it also presents serious cybersecurity and data security issues that leave companies vulnerable and open to data breaches or other cyber incidents. For starters, unsecure Internet connections—especially public Wi-Fi—can leave workers' remote devices susceptible to cyber-attacks. Physical security is also a significant risk, as employees may misplace or lose their mobile devices, allowing them to fall directly into the hands of malicious actors. In addition, remote working increases the risk of insider threats, as being away from the office considerably enhances employees' opportunities to steal data for financial gain or other personal benefit.

COMPLIANCE STEPS

To protect against the elevated security and cyber risk that goes hand-in-hand with remote working, companies should consider the following best practices:

- Cybersecurity/Data Security Policies: Companies should ensure they have cybersecurity and data security policies in place that directly address remote working. Important policies to have specifically as it relates remote working include systems access, physical access, acceptable use, removable media, mobile device/bring-your-own-

device ("BYOD"), Internet use, e-mail use, and wireless communication policies. In addition, companies must ensure that these policies are clearly communicated to all employees who will be working outside the office, and are readily accessible to all members of the organization.

- **Incident Response/Disaster Recovery Plans:** With the increased security risk that exists with remote working, it is critical that companies maintain incident response and disaster recovery plans that can be implemented immediately with adequate resources to respond to a data breach or other cyber incident. Companies should also review their plans with key personnel to ensure that everyone is up-to-speed on their roles and responsibilities in the event the plan needs to be put into action. It is important to know how to contact key personnel and members of the incident response team if they are not working on-site or if normal communications channels are not available. Realize that law enforcement may not be available to give the assistance they normally would.

- **Employee Education:** Companies must impress on their workforces the importance of proper employee data security habits, and fully educate employees on how to safely and securely use, transfer, and store sensitive company data while working outside of the office. In addition, as there has been a significant spike in phishing attacks disguised as providing coronavirus-related health information, employees should be advised to be on high alert for coronavirus-themed phishing attacks, and given guidance on how to spot attempted phishing attacks and best practices to follow. For additional information how to guard against the significant risk of coronavirus-themed phishing attacks, please view our COVID-19 Task Force's article on this topic here.

- **Virtual Private Networks:** Virtual private networks ("VPN") are a key piece of technology that add an extra layer of security by creating a safe, encrypted connections—a private network—from less secure, public Internet connections. As such, companies that have VPNs in place should ensure that employees access company networks, systems, and data remotely by using the VPN whenever possible.

- **Password Practices:** Companies should require multi-factor password authentication for access to all remote devices, which is critical to limiting potential damage when credentials or devices themselves are lost or stolen. In addition, all "remember my password" functions should be disabled on devices and applications that allow employees to access company networks and systems remotely.

- **Mobile Device Management:** Companies should consider utilizing mobile device management ("MDM") software to increase the level of security on employees' mobile devices. MDM tools allow companies to monitor, manage, and secure employees' devices that hold company data and provide the vital ability to remotely activate a range of security measures, including the wiping the data on devices if they are lost or stolen.

- **User Access Restrictions and Control:** Companies should consider restricting access to sensitive data by remote workers and adhering to the principle of least privilege, in which employees are granted only the minimal level of access or privilege that is necessary for them to carry out their job duties and responsibilities. By ensuring that employees only have access to data that is essential to their jobs, companies can significantly limit the scope of their potential attack surface, which, in turn, can significantly decrease the likelihood that they will experience a data breach or other cyber incident.

- **Public Wi-Fi Bans:** Public Wi-Fi networks are one of the most common attack vectors for cyber criminals due to their lack of security, which makes it extremely easy to intercept credentials and data over these networks. As such, companies should strongly consider banning employees from accessing their networks, systems, and data through the use of public Wi-Fi.

THE FINAL WORD

Remote working may soon become a necessity if local, state, or national quarantines are imposed, and movement is restricted except for absolutely essential purposes. Furthermore, even if no mandatory lockdowns are enacted, many businesses are considering permitting employees to work remotely to protect the health and wellbeing of their workforces while the coronavirus epidemic persists.

If you are considering implementing any type of remote work arrangements, you should speak with experienced legal counsel to ensure that your organization has in place the proper policies and practices that will ensure the security of your company networks, systems, and data while employees work from outside the office. And if your organization suffers a security incident, legal counsel can assist with managing your response.

As part of its COVID-19 Task Force, Blank Rome's cybersecurity and privacy professionals can assist with providing key counseling and guidance with respect to any issues or concerns relating to remote working considerations. And if your business suffers a security incident during the ongoing public health crisis, Blank Rome's data breach incident response team is available 24/7 and can provide immediate assistance with rapid response and crisis management following any type of breach or security event.

For additional information, please contact:

Jennifer J. Daniels, Pittsburgh Office
Partner, Cybersecurity & Data Privacy
412.932.2754 | daniels@blankrome.com

David J. Oberly, Cincinnati Office
Associate, Cybersecurity & Data Privacy,
Privacy Class Action Defense
513.362.8711 | doberly@blankrome.com