PUBLICATION

Don't Forget About Cyber Hygiene During Coronavirus (COVID-19) Outbreak

Authors: Alisa L. Chestler
March 17, 2020

As organizations prepare for certain contingency work arrangements in response to the coronavirus (COVID-19) outbreak, companies must also focus attention on ensuring appropriate cyber hygiene. Companies are anticipating more individuals working remotely from the safety of their own homes to avoid contracting the virus and other companies are planning for potential quarantines and school closings. The flexibility of working remotely, however, involves real cybersecurity risks that companies should be aware of and work to mitigate in the face of the COVID-19 outbreak. With increased remote work, there is increased risk of employees accessing data through unsecured and unsafe Wi-Fi networks, using personal devices to perform work, and not following general security protocols established by the company. As individuals are approved or otherwise authorized to work remotely, there must be a multi-departmental focus on maintaining proper controls. Management should be coordinating with the Human Resources (HR) and Information Technology (IT) departments to establish security controls and ensure employees are properly trained on those controls in the remote work context.

Companies should have a protocol in place for secured remote access to company networks. Where possible, such connections should be through a virtual private network (VPN), which routes the connections through the company's private network, or another encrypted connection mechanism. Where employees can remotely access sensitive information on the network, VPNs should be configured with multi-factor authentication (MFA) as an added security layer. With MFA enabled, even if an employee's VPN credentials are compromised, an unauthorized actor will be unable to connect through the VPN without a second factor (i.e., a code sent to an individual's smartphone, token, biometric verification, etc.). The IT Department should ensure firewalls are properly configured and monitor firewall logging to identify attempted or successful connections from unauthorized or suspicious Internet Protocol (IP) addresses. If there are regions of the country and/or world from which employees would have no reason to be remotely connected to the company network, the IT Department can proactively "blacklist" the IP ranges for those geographic regions to prevent connections. This may not be possible for a multinational company where employees may be scattered throughout the world but can be an effective measure for smaller companies or those with a regional presence.

Personal devices are more likely to be used when employees are working remotely, and such use presents additional cybersecurity risks given the lack of corporate control over the devices. Where mobile devices (i.e., mobile phone, tablets, laptops, etc.) are permitted to connect to the corporate network, companies should ensure those devices are equipped with mobile device management (MDM) software. MDM software allows the corporate IT Department to manage such devices by ensuring that the devices are configured to consistent standards, scheduling updates and patches for the devices and applications contained thereon, tracking location of devices, and – in circumstances where such devices are lost or stolen – permitting the devices to be remotely wiped.

Prior to authorizing remote connection to the corporate network, employees should have adequate training on acceptable use policies, the logistics of connecting to the network, appropriate use of Wi-Fi, and steps to take if a security incident or other compromise is suspected or identified. While these subjects are often covered in annual employee trainings, if your company is seeing increased remote work, now is a good opportunity to

provide a training update or informal security reminders. Regardless of the efforts of the company and the sophisticated security measures put in place to create a safe environment for remote workers, the risk of human error will always exist.

As your company takes steps to promote physical health in the face of the COVID-19 outbreak, you should also consider how your company can enhance cybersecurity through proper security controls and employee training. It is important to remember that all companies are different, and varying controls and procedures may be appropriate depending on the size and complexity of the company, as well as the sensitivity of the information maintained by the company. If you have any questions regarding these issues or how your organization can improve its security posture, please contact Alisa Chestler or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team. Also, please visit our Coronavirus (COVID-19): What You Need to Know information page on our website.