COVID-19 and the Increased Cybersecurity Risk in a Work-From-Home World

S. Wilson Quick
March 24, 2020

As COVID-19 has spread throughout the world and within the United States, companies of all sizes have had to make quick decisions about how to implement work-from-home procedures. While many businesses are accustomed to having some of their employees work remotely at any given time, the sudden shift to a majority of the work force being away from controlled office networks and environments presents a unique and heightened set of technical and cybersecurity challenges. Below are a few key considerations that businesses who have made or are trying to make the shift to a work-from-home arrangement in light of the COVID-19 pandemic should have front-of-mind.

Remote Access Technologies: Ensure that remote access protocols (such as virtual private networks and other remote access technologies) are properly configured, updated and ready to be deployed on a large scale. We recommend strong password protocols and at least two-factor authentication for remote access wherever possible to ensure heightened protections for the network. Also consider whether systems or programs that are traditionally only accessible from inside the office need to be made available through remote access and, if so, whether additional security controls need to be in place for particularly sensitive systems.

Proper Access Controls: Regardless of whether employees are working remotely or on site, it is important to review your network access levels to ensure that employees may only access information based on the needs of their position. Open access to all data on the network is never a good idea, but the need for heightened security is exacerbated under the current circumstances.

Use of Personal Devices: It is inevitable that employees will use their own devices to work from home over the coming

weeks—from checking email while watching the kids in the backyard to using personal tablets to videoconference, the scenarios are virtually endless. Remind employees of your bring your own device (BYOD) policy or implement one if you don't have one in place already. Among other things, strong policies should define acceptable use of devices for work purposes, provide for minimum security controls and discuss company rights for altering the device—such as remote wiping for lost or stolen devices.

IT Resources: Be cognizant that your IT staff is likely to be overworked during the pendency of the pandemic. From responding to calls about how to get videoconferencing working to dealing with the need for increased network testing and monitoring, these key members of your staff will be busier than ever before. Consider how best to deploy your limited human resources in order to maximize security efforts, while minimizing work stoppage or slow-down as employees adjust to the challenges of work-from-home. In many instances this may mean divisions in labor or bringing in trusted third-parties to help get systems up and running as quickly as possible.

Increases in Cyber Threats: As if implementing technical measures to make work-from-home a possibility is not enough, the current state of upheaval presents an irresistible target to bad-actors around the world. Cybersecurity experts from the FBI have already warned of a significant spike in COVID-19 related scams over the past week and expect the trend to continue for the duration of the pandemic. Bad actors will stoop to any level to steal your data and/or your money—from COVID-19 related phishing attacks that lead to the installation of malware or ransomware to websites purporting to sell COVID-19 "vaccines" for your employees. Companies should be aware of this reality and should proactively and regularly remind employees to remain vigilant, particularly as more and more personal devices are added to the network. In addition, consider implementing security measures to help prevent such scams, such as warning banners that identify emails from external sources.

Review Existing Policies and the Incident Response Plan: Review and update your existing privacy and information security policies and your incident response plan in light of your work-from-home arrangements. Make updates where necessary and, if no relevant policy or plan exists, put appropriate guidelines in place. Data breach and similar incident response plans should be updated, at the least, to ensure that you have updated contact information for your incident response team and any trusted outside advisors.

None of us have a crystal ball, but it appears that restrictions against gathering in one place and "shelter in place" orders may be with us for weeks—if not months—to come. Weathering the storm of COVID-19 will not be easy for any of us, but thinking through these measures and implementing well-thought-out cybersecurity protocols will help companies long beyond when the pandemic has ended.

Brooks Pierce is dedicated to keeping our clients fully informed during the COVID-19 crisis. For more information, please visit our COVID-19 Response Resources page.