Working From Home? Please Practice Good Cyber-Hygiene!

By Joseph V. DeMarco

As corporations and even entire municipalities are increasingly advising their employees to work from home in light of COVID-19, it is important to remember that doing so it not without its risks.

For any organization that has information to protect -- be it is customer or employee personally identifying information, financial information, or confidential and proprietary trade secrets -- permitting company data to travel home with or be remotely accessed by employees raises the chances of a cyber-incident involving that data. And, where a "cyber-mishap" occurs, the company may have a duty to report the incident to consumers, regulators and business counterparties. Put simply, cyber criminals are not expected to take a "corona-holiday." In fact, some might even prey on vulnerabilities created by the situation. Fortunately, there still is time to address the potential privacy and data security risks — and to develop clear guidance for employees to follow. These policies should be tailed to each company's specific risk profile and communicated clearly to all employees.

While every organization's information security defenses are unique, some of the most common risks to be addressed concerning remote work include the following:

- **Unsecure personal and public WiFi networks**: Employees' home networks and connected devices may be vulnerable to malware or ransomware attacks through their wireless router. Hackers could monitor network traffic or access files that on connected devices. In a pinch, employees might even use their personal computers on public networks at libraries or cafes, which are even less secure. Companies should therefore strongly recommend that their employees secure their home WiFi networks (which should be updated regularly) with a robust password and, when possible, employees should not use computers containing sensitive information on public networks.

- **Working on unsecure personal devices**: Home computers may be shared among family members and may not be the most up to date. They may lack critical security patch management that would otherwise protect them and the data on them. They may be laptops which are transported in vehicles and may not be password protected (or have weak or compromised passwords) and the hard drive may not be encrypted. To the maximum degree possible, employees should be advised to only conduct work on their employer-issued computers. Where this is not possible home computers should, to the greatest degree possible, be as secured as their business laptops and desktops and personal laptops should not be allowed to leave the home.

- **Transferring corporate data using personal e-mail accounts**: Employees may send sensitive information to their personal e-mail accounts, perhaps out of convenience to download on to a personal computer or to print at home. Many major webmail providers have, however, suffered data breaches in recent years and these non-enterprise email accounts usually lack the robust protections that centrally-managed commercial accounts often have, such as multi-factor authentication or logs that would help a forensic investigator determine the cause and scope of a breach. In addition to advising employees against sending sensitive company data to their personal email accounts, it is just as important to remind employees to permanently delete any corporate data remaining on their email accounts after they return to their normal working arrangement. It may even be appropriate, subject to applicable law and corporate policies consented to by the employee, to monitor company email systems to identify specific employees who have sent emails to their personal accounts and to counsel them in connection with this poor practice.

- **Synching with personal cloud storage accounts**: Employees working remotely or from home may be tempted to use a personal cloud service account to transfer documents or data to and from office that may be less secure. Files may even be synching from the employee's personal computer to the cloud without their knowledge. As with personal email, information security should monitor network activity and employees should be advised to search these accounts for any work-related data on the personal cloud accounts and permanently delete it.

- **Physical document management and destruction**: Don't forget the paper! In a hurry to migrate to a home environment, employees may take hard-copy sensitive or confidential materials off-site that they would not otherwise. They may also print hard-copy documents containing sensitive nonpublic information in public locations or on network printers with unsecure connections. Employees should be advised not to take critical materials off-site unless truly unavoidable, and to never print corporate documents at home or on hotel business centers unless the compelling reasons to do so clearly outweigh the manifest risks. Additionally, employees without cross-cut shredders at home should be advised return all printed materials once they return to the office for proper destruction and to avoid disposing of documents at home or in a public place without proper cross-cut shredding.

- **Unsecure connections to employer systems:** Absent a secure virtual private network (VPN), employees may attempt to connect to a company's systems in an insecure manner, such as using to use insecure remote desktop software to connect to their work computers. To the extent you foresee a need to access information on a company's network -- for example, many employees have a network-enabled personal drive to store their documents -- investigate the viability of configuring a VPN for certain employees or for data that is critical for conducting business. Remember also to require employees who have web access to corporate e-mail to enable two-factor authentication to the web-accessible portal or any other web-accessible corporate network.

- **Unsecure conference call lines**: An increased need for conference call or video services may exceed the capacity of the company's existing accounts. A free or online based service may seem like a sensible temporary alternative, but employees should be advised against using these for work-related calls without consulting with the company. Some services may not be secure or may even record your employees' conversations by default (a subject for another day). Employers are well-advised to proactively work with your existing – presumably secure -- conference call provider to accommodate the temporary need or identify a secure alternative for employees to use.

- **Phishing schemes and other frauds**: Unfortunately, cybercriminals are always searching for security vulnerabilities -- and opportunities -- to exploit and many employ sophisticated attacks tailored to specific organizations and their employees. A malicious hacker could target employees working from home by, for example, creating a fake coronavirus notice or phony request for charitable contributions (this happened following 9/11 and Superstorm Sandy). They might even go so far as to create a fake web page that looks exactly like the company's web-based platform to employee email and, impersonating someone in the IT department, send an email to employees with a link to the imposter site in order to harvest user names and passwords. Our firm has counseled several clients whose email systems were compromised in this manner. Employees should be advised to look out for and report any suspicious communications that appear to be impersonating someone inside the company or a trusted vendor or customer.

Because many employees are justifiably concerned for the health and safety of themselves and their families, it is understandable that data security is not their first priority as they cope with the coronavirus outbreak. However, with some careful planning, well-defined policies, and transparent communication between employees and management, companies should be able to maintain the security of their data while keeping their employees safe.