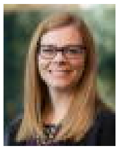
WARD AND SMITH, P.A.
ATTORNEYS AT LAW

Working Remotely and Cyber Security During the COVID-19 Outbreak

Written By Angela P. Doughty, CIPP/US (apd@wardandsmith.com) **and**
Erica B. E. Rogers (ebrogers@wardandsmith.com)
March 26, 2020



The number of positive cases of COVID-19 is rapidly increasing throughout the United States, requiring more and more employers to rely on employees working from home.

While this is a necessity under current conditions, especially as state and local government agencies *require* that we "shelter-in-place," it is not without creating other business risks such as cyber security breaches.

The work from home dynamic creates a very opportunistic situation for hackers and phishers. Every home device or wireless connection is a potential entry point. Moreover, with employees justifiably focusing on other things – their children, pets, health concerns, finances, etc. – data security is understandably not top of mind and employees' typical safeguards against cyberattacks are down. We have seen a significant rise in COVID-19-related phishing attacks, where hackers are taking advantage of individuals' fear and need for health, safety, and financial aid information. Unfortunately for businesses, a company can lose control over its data and be subject to significant legal liability due to a single email click or transmission of its data over an unsecured network. However, with appropriate planning, policies, and employee education and communication, companies can minimize risk and support their employees.

While all businesses have different cyber security risks, there are some basic precautionary steps all businesses can take:

First, companies can take advantage of employee free time by offering **updated training materials**.

From the hacker's perspective, distracted employees using personal devices and Wi-Fi connections without encryption are the ideal targets. There are more opportunities to compromise a network and obtain access to personal data, financial data, and other sensitive data.

From the employer's perspective, though, employees at home have the extra time to educate themselves on this important subject. For example, every individual should be aware of phishing attacks, where fraudulent links about COVID-19 or federal relief packages (*e.g.,* "Click here to claim your $1,200 check") are especially appealing. Deceptive emails can be avoided if employees are educated about them.

Second, companies can update their **employment information security policies**, including "bring your owr device" (BYOB) policies, to contractually protect against employee wrongdoings, including, but not limited to:

a. misuse of personal emails to send or receive company emails;
b. synching and storing business information on personal cloud accounts;
c. misuse of social media to discuss company matters;
d. misuse of personal, unsecured connections to employer systems;
e. misuse of unsecure conference lines;
f. misuse of public, unsecure wireless connections;
g. careless safekeeping of company devices in public areas, which increase the likelihood of theft;
h. misuse of easily identifiable passwords*;
i. improper disposal of paper materials containing sensitive information (*e.,* not shredded); or
j. misuse of screen-sharing on video conferences.

*Weak passwords are vulnerable to password cracking attacks. The best passwords contain many characters (fifteen) and are routinely updated. Better are multi-factor authentication passwords, for example, a password followed by an SMS message to authenticate that password with a second device.

Third, companies can adopt **security measures for employees' personal devices**.

Employers can offer up-to-date anti-virus software for employee personal devices.

Employers can ensure personal Wi-Fi wireless networks include network security technology (*e.g.,* Wireless Protected Access or "WPA2"). WPA2 is a type of encryption used to secure networks by, basically, scrambling the data to make it harder for hackers to perceive the data.

Certain software allows companies to remotely access personal devices to make updates or patches to cover vulnerabilities or to delete information should that device be lost or stolen.

Finally, companies can add banners to internal versus external emails so that employees can identify whether an email is coming from a safe source.

Fourth, companies can update or adopt a **data security breach response plan**.

Companies should review their data security breach response plan considering remote working.

State data breach notification laws sometimes require immediate action, so ensuring a plan to comply ahead of time is paramount. If any employee believes he or she is responsible for a data breach or successful phishing scheme, the correct contact person for immediate notice should be obvious.

Ward and Smith's Privacy and Data Security team routinely counsels and assists clients across a broad spectrum of industries, including finance and banking, healthcare, technology, construction, and retail with navigating the complex requirements of privacy and data security regulations and managing the risks and breach notification requirements related to data security incidents.

Please visit our Privacy and Data Security page for more information.

--
For further information regarding the issues described above, please contact Angela P. Doughty, CIPP/US or Erica B. E. Rogers.

This article is not intended to give, and should not be relied upon for, legal advice in any particular circumstance or fact situation. No action should be taken in reliance upon the information contained in this article without obtaining the advice of an attorney.

We are your established legal network with offices in Asheville, Greenville, New Bern, Raleigh, and Wilmington, NC.