ATTORNEYS AT LAW

BULKLEY RICHARDSON

BETTER REPRESENTATION

CYBERSECURITY IN REMOTE WORK ENVIRONMENTS

In the wake of COVID-19, employees that are able to work from home are doing so. This move to a remote workforce—from company-issued devices to at-home Wi-Fi, from in-person lunch meetings to large group Zoom meetings, and from a congregation to a diaspora of employees—presents many technological challenges.

It also presents opportunities for cyber criminals.

To thwart hackers that are looking to take advantage of the situation, consider implementing (or confirming that you have implemented) the following administrative and technical safeguards, consistent with 201 C.M.R. 17, in order to provide reasonable security of any personal information at your company.

Be Aware of—and Alert Your Employees to the Prevalence of—COVID-19 Specific Scams

- **Wire Transfers:** The FBI anticipates a rise in Business Email Compromise ("BEC") scams. In this scam, detailed **here**, the victim receives an email they believe to be from a legitimate vendor, but with altered wiring instructions (in one recent, successful scam, the change was justified by claiming it was "due to coronavirus outbreak and quarantine process and precautions"). Be wary of any last-minute changes in wire instructions, confirm any changes through contact information provided outside of the email altering the instructions and doublecheck the email address of any party sending these emails, particularly when you are viewing emails on a mobile device.

- **Phishing:** Phishing is a cyberattack that uses email to collect valuable information, install malware on a computer system or otherwise intrude on a business's network. It starts when an individual clicks on a link or downloads a file. **The Federal Trade Commission ("FTC")** and **Department of Homeland Security** have published alerts about and tips for avoiding these scams.

- **COVID-19 Specific Information:** Given the volume of and interest in information about COVID-19, cybercriminals have begun to incorporate COVID-19 into their phishing emails, with email subjects like "2020 Coronavirus Updates" or "2019-nCov: Coronavirus outbreak in your city (Emergency)," sometimes imitating the email address of the CDC or human resources department at your business. Cybercriminals have also begun to incorporate a link to a replica of the (excellent) interactive map from Johns Hopkins University. There are also apparently variants where the email source pretends to offer priority registration for a vaccine.

- **The Grandparent Scam:** In this scheme, the cybercriminal poses as a grandchild or other family member who needs money immediately, often for a hospital bill. Employees should be encouraged to independently contact someone who can verify this information before transferring any funds.

Secure Your Company's Expanded Network

The FTC and the **National Institute of Standards and Technology** have made the following recommendations for telework:

- Require your employees to encrypt their at-home wireless network by using WPA2/WPA3 options and password protection. Instructions can be found **here**.
- If employees are not using company-provided devices, remind them of (or develop) Bring Your Own Device policies consistent with your business's cybersecurity practices. At a minimum, consider requiring employees to use all available security (password, fingerprint authentication, etc.) specific to devices that will be used for work purposes.
- Set up two-factor authentication for access to your company's servers.
- Use a virtual public network whenever possible.
- Update company devices with anti-virus software and patches regularly and require employees to do the same with any device used to conduct company business.

> If you are experiencing a cybersecurity incident, if you would like to update your WISP to account for remote employees, or if you would like more information about complying with cybersecurity obligations in the wake of COVID-19, please contact Lauren Ostberg or Jim Duda of Bulkley Richardson's Cybersecurity practice group.

Lauren Ostberg

✉ lostberg@bulkley.com
☎ 413-272-6282

Jim Duda

✉ jduda@bulkley.com
☎ 413-272-6284