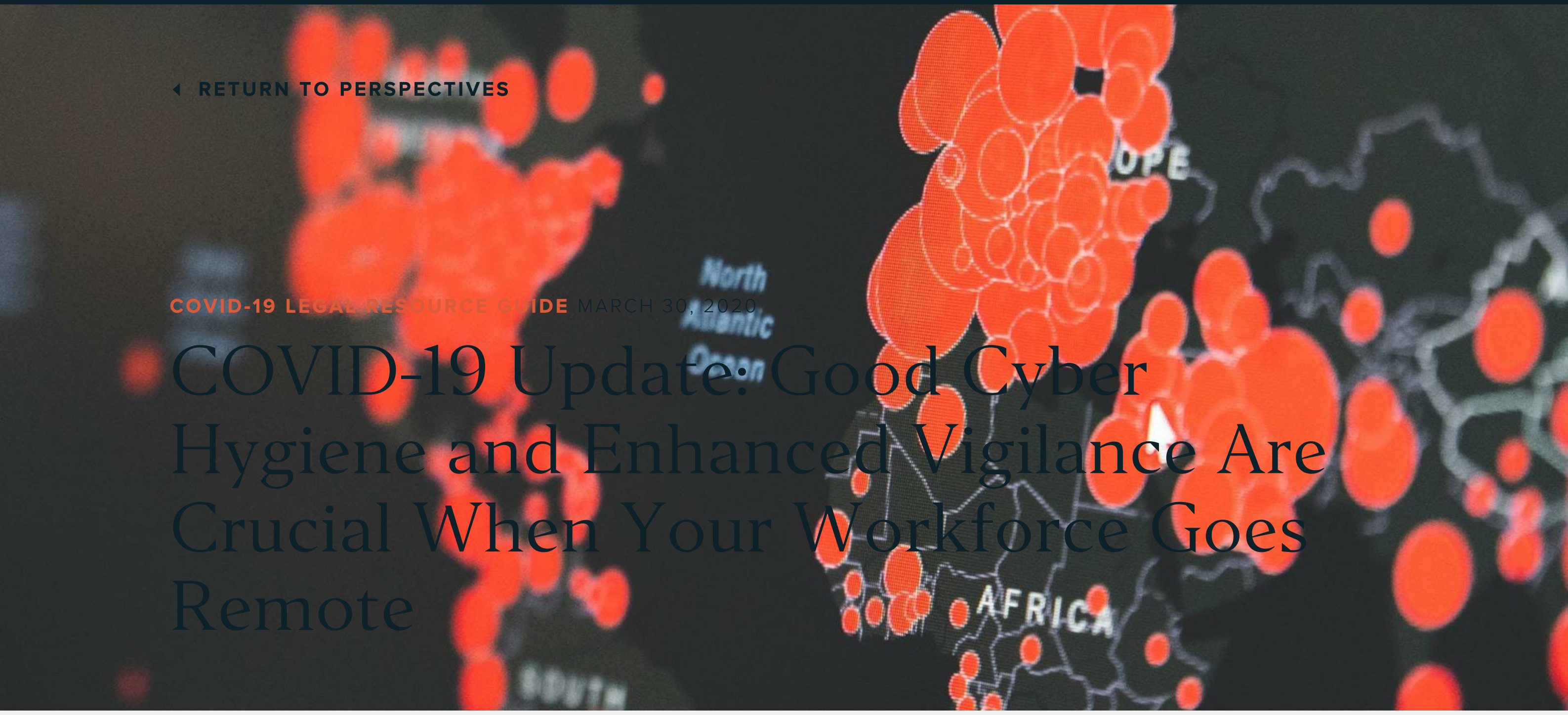

RETURN TO PERSPECTIVES

COVID-19 LEGAL RESOURCE GUIDE MARCH 30, 2020

COVID-19 Update: Good Cyber Hygiene and Enhanced Vigilance Are Crucial When Your Workforce Goes Remote

As organizations transition to the work-from-home environment, the risks of cyber fraud grow even more acute. Fraudsters are seeking to exploit remote workforces to gain access to valuable confidential and personally identifiable information, using timely phishing and man-in-the-middle scams as well as standard firewall and perimeter penetration. Consider taking these basic steps to protect your organization from cybercriminals.

Remember that many cybercrimes are accomplished through the use of email. Common email cybercrimes include phishing scams, corrupted attachments and attempts by bad actors to obtain personal or financial information or misdirect money or other items of value. Many hackers are capitalizing on coronavirus fears to obtain remote system access, such as through phishing scams that encourage recipients to click on links to purchase masks or hand sanitizer or to connect to helpful coronavirus information from reputable organizations like the Centers for Disease Control and Prevention or the World Health Organization. Fraudsters are even impersonating state and local Department of Health workers and cold-calling homes, purporting to set up Coronavirus tests in an effort to solicit personal and protected health and identifying information.

To guard against these scams, encourage the use of good email cyber hygiene habits, including:

- Scrutinizing unexpected email and telephone communications and email addresses to make sure each communication is actually from the person it appears to be from.
- Looking for suspicious typos, odd uses of grammar or other indications the email may have been drafted by a bad actor.
- Subjecting any unusual requests to additional levels of verification — e.g., calling to verify.
- Scrutinizing all links before clicking, and erring on the side of sending suspicious links or documents to the information technology department for review before opening or
- Immediately informing the information technology department if a suspicious link is clicked.
- Not forwarding documents containing confidential information to personal email accounts, which are much easier to hack.

Be alert to man-in-the-middle fraudsters seeking to exploit the remote work environment. Man-in-the-middle attacks occur when a perpetrator positions herself in a conversation between two email users to impersonate one of the parties, making it appear as if a normal exchange of information is underway. For example, a perpetrator might use a slightly different email address — e.g., CEO@compaany.com rather than CEO@company.com — to cause the person receiving the email (the victim) to send funds to an account controlled by the perpetrator rather than to the company's account.

Ways to spot and stop man-in-the-middle attacks — whether they are purporting to send money to a new or old vendor — include:

- Subjecting any unusual requests — including, for example, last-minute changes to wire or other payment instructions or other requests to deviate from normal procedures — to additional levels of scrutiny. Pick up the phone and verify.
- Creating and enforcing vendor payment procedures that include, for example, preestablished wire transfer instructions, telephone confirmation prior to transfer and other approval layers.

Be aware of the unique security concerns presented by devices with listening capability or voice activation. Advise employees to mute or shut off listening devices like Amazon Echo, Nest cameras, and Amazon's Alexa or Google's voice assistant when discussing confidential matters. These kinds of devices present a myriad of security issues:

- Studies show that the recording feature of these devices can be inadvertently activated numerous times throughout a single day.
- The devices also have been known to inadvertently forward recorded conversations.
- Tech companies have come under fire for listening in on users' conversations in furtherance of improving their artificial intelligence technology.
- Hackers can breach these systems to monitor conversations for valuable information.

Take into account cybersecurity and data privacy issues when determining whether and how to rely on vendors or other third parties to manage the new burdens imposed by the work-from-home environment. Consider, for example:

- Are the cyber safeguards implemented by the vendor adequate to protect company data?
- Does the transfer comply with all applicable data privacy laws?
- If the transferred data has been entrusted to the company by another party, does the transfer comply with that party's expectations and requirements?
- Are employees employing good cyber practices — including password protection and encryption in transit — in connection with the transfer?

Make sure all devices have secure passwords. Experts advise that passwords be at least 12 digits in length, with symbols, numbers, letters and varying use of capitalization — e.g., Pe@nut$_&_cr@ckerj@ck$.

Overall heightened vigilance, frequent reminders of good cyber hygiene and related company policies, and good common sense will serve your company well.

AUTHORS AND EDITORS

Alan R. Friedman
Partner
New York

afriedman@kramerlevin.com
T 212.715.9300
F 212.715.8300
VCARD

Samantha V. Ettari
Special Counsel
New York

settari@kramerlevin.com
T 212.715.9395
F 212.715.8406
VCARD