Lowenstein Sandler

Privacy & Cybersecurity

April 16, 2020

COVID-19 Era Remote Work Environments Increase Cybersecurity Risks: What You Need to Know and Do

By Mary J. Hildebrand CIPP/US/E, Edgar R. Hidalgo CIPP/US, and Carly S. Penner CIPP/US

In response to the COVID-19 pandemic, significant sectors of the global workforce abruptly shifted to working remotely. Private and public businesses, government operations, and educational institutions moved en masse to home-based work environments. This unprecedented disruption stressed not only the millions of individuals involved, but also the complex technology infrastructures that were suddenly required to accommodate massive traffic volumes. As with any major disruption, COVID-19 has encouraged innovation to meet rapidly changing needs. However, among the many constructive responses to the pandemic, there are also hackers and bad actors who see an opportunity to exploit security weaknesses in the technology infrastructure supporting the newly decentralized workforce. Businesses that have implemented remote working infrastructures need to take steps to minimize exposure from these increasing cybersecurity risks.

Remote Working Environments

While social distancing, lock-downs, and remote working are a cornerstone of the global fight against COVID-19, adopting these practices has exposed businesses to heightened cybersecurity risks. Among the causes frequently cited are that IT resources have been deployed to address system bandwidth issues and server capacity for the remote workforce at the expense of cybersecurity. Additionally, short notice of shelter-in-place orders has left many businesses scrambling to purchase, and provide workers with access to, company-issued laptops and/or security software at a time of soaring demand. Organizations have also been compelled to quickly expand or even establish new relationships with third-party vendors and platforms to support the remote workforce, often with insufficient time to conduct privacy and security diligence or provide current training suitable for the new model.

As businesses struggle to adapt, employees often resort to using their personal devices and accounts to communicate (internally and externally) by email, especially in the context of communicating about COVID-19. These personal devices and accounts may not have security measures in place comparable to those in the business' primary IT system. Additionally, many employees have little or no experience with remote work and communications, and may not be sensitized to the potential repercussions of sharing personal, confidential, or business information through unsecure networks. Thus, the incredibly rapid implementation of remote working, while socially responsible, has made individual employees, and therefore the organizations that employ them, more susceptible to targeted phishing, fraud, and malware attacks.

National and Global Warnings

Cyberattack perpetrators are well aware of the vulnerabilities of these remote working environments. Since the onset of the COVID-19 pandemic, the U.S. government and global organizations have released urgent warnings regarding a spike in phishing, fraud, and other cyberattacks. The Cybersecurity and Infrastructure Security Agency in the Department of Homeland Security warned the public that cyber actors might use COVID-19-focused emails with malicious attachments or links to fraudulent websites. The FBI's Internet

Crime Complaint Center has cited ongoing phishing attacks using the CARES Act and other economic stimulus legislation to bait individuals with false information and the promise of easily obtained loans or cash grants. In similar swindles, the World Health Organization has discovered ongoing coronavirus-themed phishing attacks in which the perpetrators impersonate WHO representatives to access sensitive personal information and infect equipment with malware. On March 31, the U.S. Federal Trade Commission reported that consumer fraud complaints related to COVID-19 have surged since the beginning of the year. In a welcome development, the United States Department of Justice has made enforcement against bad actors taking advantage of the pandemic a priority. "The pandemic is dangerous enough without wrongdoers seeking to profit from public panic, and this sort of conduct cannot be tolerated," Attorney General William Barr wrote in a March 16 internal memo to all U.S. attorneys general.

Regulatory Guidance

Regulators have noted the increase in cyberattacks and other nefarious cyber activity, and identified remote working arrangements as a key factor encouraging such actions. Further guidance is likely to be released in the near term. The Consumer Financial Protection Bureau and Federal Trade Commission are actively engaged in gathering information regarding the measures that financial institutions, financial servicers, and vendors are taking to protect consumers' nonpublic personal information while relying on largely remote professional and administrative employees. While we do not anticipate that most federal regulators will relax enforcement of security rules under federal law, the Department of Health and Human Services has scaled back on enforcement of applicable rules under the Health Insurance Portability and Accountability Act in connection with telehealth providers and first responders. Still, indications are that all federal regulators are aware of the challenges involved in ensuring that remote working practices remain in compliance. At the state level, on April 13, the New York Department of Financial Services issued guidance to regulated entities on how to ensure their remote working processes and systems remain compliant with existing cybersecurity requirements.

Steps to Mitigate Risk

During the initial phase of remote working, businesses are understandably focused on continuing operations with minimal disruption. As recent experiences have shown, however, business priorities should include taking steps to mitigate the attendant risks of cyberattacks. All relevant stakeholders across the business should be involved in these efforts:

- *Employee Engagement and Training*. Alert your employees regarding the enhanced cybersecurity risk and conduct appropriate training in connection with the remote working environment—and then do it again.
- *Update Internal Security Policies.* Revise internal security practices and polices including provisions for remote work environments; practices and policies for using personal devices remotely, including, as applicable, prior approval of devices; installation of applications to protect or wipe business data from the device; and other security measures.
- *Tailor Incident Response*. Update incident response plans, disaster recovery plans, and other data security plans to include your remote workforce, and conduct remote working tabletop exercises with your cybersecurity teams.
- *Revisit Insurance Coverage*. Analyze current cyber insurance policies to ensure coverage extends to your remote workforce.
- *Diligence Vendors*. Evaluate third-party vendor dependencies that support remote working, including an appropriately scaled security diligence process.

To see our prior alerts and other material related to the pandemic, please visit the Coronavirus/ COVID-19: Facts, Insights & Resources page of our website by clicking here.

About Us

In today's digital world, where data has become a key asset for conducting business, companies continue to face greater privacy and cybersecurity challenges. At Lowenstein Sandler, our Privacy & Cybersecurity team helps clients navigate the rapidly evolving, increasingly complex privacy and security law landscape in the United States, the EU, and around the world. We deliver innovative privacy and security solutions that meet our clients' critical business needs including the commercialization of data assets in a legally compliant manner. Our targeted counsel is relevant to companies across diverse industry sectors, and public and private companies from start-ups to global enterprises..

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

MARY J. HILDEBRAND CIPP/US/E
Partner
Chair, Privacy & Cybersecurity
T: 973.597.6308
mhildebrand@lowenstein.com

EDGAR R. HIDALGO CIPP/US
Counsel
T: 973.422.6418
ehidalgo@lowenstein.com

CARLY S. PENNER CIPP/US
Associate
T: 973.597.2516
cpenner@lowenstein.com