Cybersecurity for a Remote Workforce

March 24, 2020

Coronavirus (COVID-19) has prompted a rush by many organizations to a remote working environment. This alert outlines key security considerations for remote work, plus some resources. As the crisis ebbs, this abrupt expansion of remote work will likely produce many positive workplace changes. In the meantime, opportunists search for vulnerabilities to exploit, and remote work needs to be as secure as possible.

SANS, a non-profit security-awareness organization, recently issued a five-point handout for employees about to work at home. By far, the greatest threats are phishing and other social engineering methods aimed at employees worried about COVID-19. One successful link mimics a COVID-19 tracking map.[1] Coronavirus-related domains are currently 50% more likely to be malicious than other domains.[2] Homeland Security (DHS) reminds users to "[e]xercise caution in handling any email with a COVID-19-related subject line, attachment or hyperlink, and be wary of social media pleas, texts or calls related to COVID-19."[3]

The Cybersecurity and Infrastructure Security Agency (CISA) of DHS just issued a list of insights for executives seeking to implement a remote workplace. It suggests strategies to protect infrastructure, supply chains and data from attack in a remote environment.

Organizations with remote workers should consider these specific measures:

- Establish clear rules for remote work, and change existing policies as needed.
- Use a Virtual Private Network (VPN) for network access.
- Check VPN logs for irregular usage patterns indicating compromised accounts.
- Impose multifactor authentication.
- Survey employees on their home wifi networks and explain how to secure them.
- Adopt a mobile device management (MDM) app for connected personal devices, allowing for tracking, shutdown and remote wiping of data as necessary.
- Employ good computer hygiene.
    - Encrypt hard drives, devices, data as possible and feasible.
    - Patch software and keep antivirus protections up to date.

- Require (and force periodic changes to) strong passwords.
- Limit user privileges and credentials, especially to sensitive data.
- Utilize automatic lockouts and screensavers to keep family out.
- Prohibit the use of flashdrives and other external storage devices.
- Preclude use of personal email or cloud accounts (*g*, Dropbox/iCloud) for company information.

These measures address existential threats to a business. Ransomware remains a potential gamebreaker for companies already stretched to the limit by the COVID-19 pandemic. On March 14, 2020, for example, the Champaign-Urbana Public Health District paid a $350,000 ransom to retrieve its files. "We believe hackers target organizations when they are most vulnerable. With the current Covid-19 outbreak we didn't waste any time," the District's HR Director told the Wall St. Journal.[4] A company should separate, or "gap" its backups so that malware in its network cannot reach it.

Companies should have in place up-to-date Business Continuity, Disaster Recovery and Incident Response plans. If not, our cybersecurity team of attorneys can create, revise or help practice ("tabletop") them. We also help businesses comply with the growing number of new obligations from data privacy and security laws in California, New York, Massachusetts and other states and countries.

The coronavirus pandemic has imposed massive changes to the workplace and the global economy. By utilizing appropriate cybersecurity measures, an organization can focus on its core business operations and prepare for a future that will undoubtedly include more remote work.

For more information, contact Tedrick Housh or Michael Cohen from our Global Privacy, Cybersecurity & Data Protection team or your Lathrop GPM attorney.

[1] See https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/

[2] See https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/

[3] See https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams

[4] See https://www.wsj.com/articles/hackers-target-medical-providers-to-exploit-coronavirus-uncertainty-11584552411