PAUL HASTINGS

STAY CURRENT

March 2020

Follow @Paul_Hastings

PH COVID-19 Client Alert Series: The Cybersecurity Implications of an Entire Organization Working from Home

By Robert Silvers, Bianca Ponziani & John Binkley

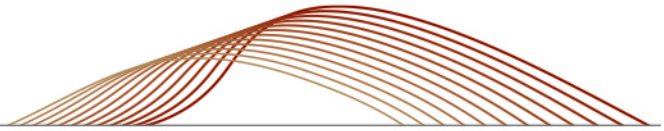
As organizations continue to monitor the Coronavirus ("COVID-19"), many have announced work-from-home ("telework") policies to mitigate the spread of the outbreak. The scope and speed at which entire workforces have gone remote pose complex challenges for organizations that may not be prepared for, nor maintain the hardware or software to accommodate, a wholly remote operation. Most companies were not built for this, and need to ensure their surge migration to remote working is executed securely.

Safeguard Sensitive Information Off-site

As a practical matter, organizations should not assume that their workers have access to reliable internet connections or a connection with sufficient bandwidth to support popular video-conferencing and collaborative software programs. Those that do have reliable internet access may be working on an unsecured network or a network whose capacity may be diminished by the simultaneous internet-based activities of family members or housemates who are also self-isolating.

Now is the time for organizations to enhance their cybersecurity hygiene by reminding employees that sensitive information must only be accessed through secure networks, even while at home; sending confidential information to a personal inbox for ease of printing, for instance, may only accomplish the task at the expense of system-wide harm. Further, employees will likely be handling physical documents containing sensitive information at home, sometimes without access to a locked storage cabinet, posing challenges to compliance with legal regimes like HIPAA and financial services regulations. To preempt employees taking less secure shortcuts, and to minimize the risk of disclosure of physical documents, organizations may consider:

- Adequately resourcing information technology ("IT") help desks to handle increased requests for remote access assistance.
- Employee verification tools for requests issued by phone.
- Sending reminders of (or developing, if needed) internal policies governing the proper handling and disposal of documents containing sensitive information.



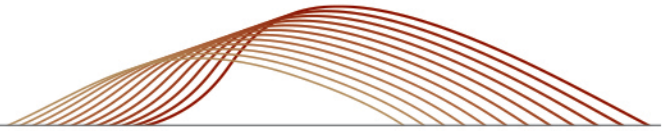
- Teaching workers how to secure their home Wi-Fi network and how to identify an unsafe Wi-Fi network or a network that may not be configured correctly.
- Providing organization-owned and managed equipment with proper endpoint protection and virtual private network ("VPN") software, for those working remotely.
- If personal devices must be used, provide remote workers with free access to endpoint protection, VPN, and approved communication systems to provide some level of validation and assurance of security.
- Maximize the use of organization-managed cloud services delivered through browsers such as Office 365, Google Docs, Microsoft Teams, Slack, etc.

Expect Cybercrime Exploiting the COVID-19 Pandemic

Unfortunately, yet as expected, cybercrime has escalated very quickly to exploit the understandable fear surrounding COVID-19, as we reported here. There are widespread reports of phishing emails disguised as alerts sent by the U.S. Centers for Disease Control and Prevention and the World Health Organization, tailored to recipients' locations. In one instance, a cybercriminal capitalized on the COVID-19 outbreak by using pandemic-specific messaging to cause predominantly Japan-based recipients to download malware that appeared to have been sent by a provincial health authority.

Organizations should recurrently educate their workforce on techniques to identify suspicious correspondence, including on social media platforms, which are intended to install malware or illegitimately obtain employee usernames and passwords. To this end, proactive steps include:

- Requiring employee training on the signs of a phishing campaign, such as "lookalike domains" (e.g., the letter "i" may be replaced with the digit "1"), spelling errors, and unfamiliar senders.
- Announcing any increased rate of cyber or phishing attacks to keep the risk top of mind.
- Circulating internal COVID-19 alerts using one consistent layout without links or attachments, which will make it easier to spot phishing attempts that do not conform to the organization's alert format.
- The use of multi-factor authentication to access software programs and devices can help protect against the impacts of login credentials stolen through phishing.
- Circulating a best practices document for company devices (e.g. strong passwords), bring your own device ("BYOD") programs (especially relevant to organizations that do not have a sufficient number of company devices to issue to each employee), and the use of mobile devices for professional purposes.
- Provide remote users using personal equipment free access to endpoint protection software that includes features such as antimalware software, application whitelisting, host-based firewall, and host-based intrusion detection and prevention systems.



Shore up IT Systems Ahead of a Cyber-incident

To comply with the wide variety of regulatory regimes that impose security standards, corporate information security teams, must take fast action to fortify the company's infrastructure. This applies to consumer-facing businesses subject, for example, to the Federal Trade Commission Act or the California Consumer Privacy Act, both of which require companies to maintain reasonable security controls. In addition, certain regulators have directed companies to develop a business continuity plan to respond to the disruptions expected from COVID-19. The New York State Department of Financial Services ("DFS"), for instance, issued guidance for institutions to put in place and submit to DFS "preparedness plans to address operational risk posed by" COVID-19, to include cybersecurity, that reflect the institution's relative size, complexity, and activities. The guidance states expressly that boards of directors and senior management are responsible, respectively, for allocating sufficient resources to implement and putting in place effective procedures to execute such plans.

A preparedness plan to protect remote accessibility will generally include at least the following components:

- Regular updates to both VPN and remote desktop systems with the latest software and security patches.
- Tests to ensure enterprise VPN and remote desktop systems can handle an entire workforce, and selecting alternatives to accommodate excess demand that do not compromise IT security.
- Revisiting crisis management and incident response plans to identify whether the plan can be executed by a remote workforce. Key personnel may be off-site or unavailable for the duration of the outbreak. Companies should test, through tabletop exercise simulations, whether they are prepared to respond to a serious incident on that basis.
- Opening lines of communication with cybersecurity vendors to address any foreseen impacts of COVID-19 on their ability to provide critical support in the event of a cybersecurity incident.

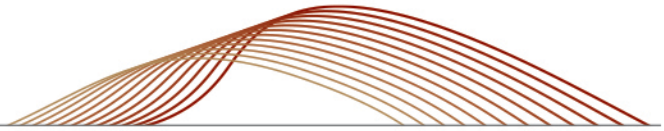
Staying Informed and Complying with Applicable Laws

Tools that organizations can use to stay current on cyber-related threats include subscriptions to, for example, the U.S. Cybersecurity and Infrastructure Security Agency ("CISA") alert service, guidance from information sharing and analysis sectors that cover your company's industry sector, and threat intelligence feeds from cybersecurity companies.

As discussions related to personal health continue to take place during this outbreak, particularly between employees and employers, organizations must ensure that communications involving employee protected health information is handled pursuant to applicable privacy laws as we described in further detail here.

It is unclear when we will all be back in the office. We need to secure the new working environment we will all be operating in for the foreseeable future; regulators are expecting it, and hackers are only accelerating their efforts to take advantage.

✧ ✧ ✧



If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

New York

Bianca G. Ponziani
1.212.318.6757
biancaponziani@paulhastings.com

Washington, D.C.

Robert P. Silvers
1.202.551.1216
robertsilvers@paulhastings.com

John Edward Binkley
1.202.551.1862
johnbinkley@paulhastings.com