SULLIVAN & CROMWELL LLP

March 30, 2020

Heightened Cybersecurity Risks Resulting From COVID-19's Effects on Operations

Companies Should Be Alert to Cybercriminals Exploiting Remote Working Vulnerabilities and Interest in COVID-19

SUMMARY

Cybersecurity risks have increased substantially as companies across the globe have shifted to employees working remotely as a result of the COVID-19 pandemic. Companies must balance these risks, upon which cybercriminals are seeking to capitalize, against the companies' need to operate remotely. In this memorandum, we identify cybersecurity threats that have been shown to be heightened in times of public crisis, and which have already been deployed against companies and individuals in the wake of the COVID-19 pandemic. We also identify measures companies and individuals can take to protect against these threats.

Specifically, cybercriminals have been sending phishing emails (designed to gain unauthorized access to employees' email accounts and the company's computer network) that purport to provide information about COVID-19. Cybercriminals have also begun launching "business email compromise" schemes (designed to deceive employees with control over company financial accounts to send money to the perpetrators in response to what appear to be legitimate email requests) using emails that reference a supposed urgent company need to pay for certain goods or services in response to the COVID-19 pandemic. Cybercriminals are also expected to capitalize on the current remote work environment by impersonating employees and IT administrators in phone calls and emails in an effort to gain access to employees' network credentials and the company's network. To protect against these threats, companies should educate and sensitize the workforce to them, consider reviewing and updating information security policies, and crisis management and incident response plans, and ensure that crucial data is securely copied and stored in an off-network location.

HEIGHTENED CYBERSECURITY RISKS

Many of the cybersecurity threats that companies face in connection with COVID-19 are well-known schemes that are being re-tooled and tailored to target employees who are still becoming accustomed to working remotely and individuals who are seeking current information and guidance about COVID-19.

- ***Phishing Emails*.** Phishing emails are designed to appear like legitimate emails, but deliver malicious software, or malware, to infect a victim's computer or network, usually when the victim clicks on a link or attachment to the email. The malware delivered by phishing emails is the source of a substantial amount of all cybercrime, enabling the perpetrators to steal money or information, to destroy networks, and to launch ransomware attacks that encrypt computer data, rendering it useless, unless the victim pays a ransom.

  In the current climate, in which legitimate information about COVID-19 is being widely disseminated and there is acute public interest in that information, individuals may be less sensitive to opening and clicking on links in emails from sources they do not recognize. Cybercriminals are capitalizing on this reality by sending waves of malicious phishing emails that purport to provide information about COVID-19.

  For instance, the World Health Organization ("WHO") has warned that cybercriminals are sending COVID-19-related phishing emails impersonating the WHO or WHO officials,[1] and the FBI has alerted the public that cybercriminals are sending phishing emails that purport to be from the Centers for Disease Control and Prevention, to seek charitable donations, to offer airline refunds, or to provide information about cures, vaccines, or testing kits.[2] More broadly, there has been a reported increase in the registration of COVID-19-related websites being used to host phishing attacks.[3]

  One reported COVID-19-related phishing scheme involved an email that included, as an attachment, a document recounting what appeared to be legitimate advice for protecting oneself from COVID-19. When opened, however, the document loaded malware onto the victim's computer, unbeknownst to the victim. Another reported example involved an email that superficially appeared to be sent from a company's outside contractor explaining how the contractor intended to respond to the COVID-19 pandemic, but was actually a vehicle for delivering malware.[4]

- ***Business Email Compromise*.** In a "business email compromise" ("BEC"), the perpetrator deceives the recipient into sending money to an account that the victim believes is legitimate, but is actually controlled by the perpetrator. BECs take many different forms, most commonly an email to an individual who has authorization to distribute funds for a company or another person, and who is asked to make a payment that appears otherwise legitimate. The perpetrators often make use of information that can be found on the internet about the target company and its particular executives and business partners to design highly deceptive emails that are specifically tailored to the target company's business and circumstances. For example, the email may appear to be from an actual company vendor requesting that payment be made to a new bank account, and only on close inspection can it be discovered that the address from which the email was sent is slightly different from the vendor's actual email address. BECs are extremely common and can cause enormous losses. The Department of Justice, for example, charged a defendant for deceiving finance professionals at two major U.S. technology companies into wiring $100 million in response to apparently legitimate vendor invoices requesting payment to a new, overseas bank account, which was in fact controlled by the defendant.[5]

  Because BECs are most successful when the perpetrators can persuade targets that there is an urgency to the requested payment, COVID-19 has created new opportunities for perpetrators of BEC schemes. As companies face challenges accessing credit markets, receiving goods and services, and operating remotely, employees may become more susceptible to responding to what appear to be urgent requests from executives and authorized persons to send money as directed

by email. There has been at least one reported incident of a COVID-19-related BEC in which a victim was asked to transfer funds to a different bank because of the COVID-19 pandemic.[6]

- ***Information Security Imposters.*** Cybercriminals are expected to capitalize on the vast increase in the number of employees working from home in response to COVID-19. For example, cybercriminals may impersonate a company information technology ("IT") administrator and contact employees to try to obtain or verify credentials to access the company's network, or may impersonate an employee and contact an IT administrator to gain access to the network. These questions and calls between IT personnel and employees may not strike some employees as unusual under the circumstances.
- ***Watering Hole Attacks.*** In a so-called "watering hole attack," the perpetrator creates a website infected with malware that is downloaded to victims' computers without their knowledge or permission when they visit the website. Given the interest in information about COVID-19, cybercriminals are creating malicious "watering hole" websites that purport to provide information about COVID-19 but actually deploy malware to the computers accessing the site. The FBI has stated that users should be especially cautious of websites and apps claiming to track COVID-19 cases.[7]

MEASURES COMPANIES CAN TAKE

There are steps companies can take to help protect themselves and their employees and to ensure they are less vulnerable to emerging cybersecurity threats related to COVID-19.

- ***Educate and Sensitize the Workforce.*** The Cybersecurity and Infrastructure Security Agency recently recommended that employees be alerted to the increased risk of phishing in connection with COVID-19, including that such phishing emails may purport to have important notices or updates on the COVID-19 pandemic.[8] Employees should equally be alerted to the increased risk of BECs, phone calls, or emails in which unauthorized persons try to obtain password credentials or network access, and fraudulent websites that purport to provide information related to COVID-19. A bulletin or message to all users on these subjects is helpful. Companies may also consider sending a test lure—a controlled phishing email addressing COVID-19 topics—to see who clicks on it and thus who would benefit from a reminder about these heightened cybersecurity risks.

  Individuals should also be encouraged to ensure that their personal devices, including internet routers, are current on anti-virus protection and only use secured, password-protected internet connections. In addition, individuals should maintain secure and confidential passwords, such as using long and unique passwords or by using commercially available password managers.
- ***Review Information Security Policy.*** Companies should also review their information security policy with a focus on the fact that remote working is currently the norm rather than an exception. Companies should consider whether: (i) the policy's provisions all still apply, (ii) the policy covers the risks that exist with remote working, and (iii) new security requirements should be put in place. For example, companies may consider restricting access to personal email or to public cloud-storage or file-sharing systems from company-issued devices. Remote connections with higher security standards—like encrypted Virtual Private Networks ("VPNs")—can take longer, and some employees may try to use workarounds to expedite their work, for example to print their work using a personal printer. To the extent employees are using their home Wi-Fi connections to connect to the company's network, companies should encourage employees to ensure that their Wi-Fi connections adhere to appropriate security standards, or consider using a VPN provider that will not allow a computer to connect unless certain minimum security requirements are met. Moreover, with the prevalence of video-conferences that substitute for in-person meetings, companies may want to examine device security standards for company-issued and/or personal devices, as applicable. Changes to the policy can be distributed with a cover message noting key changes and reminders.

- ***Review Crisis Management and Incident Response Plan*.** Companies' crisis management and incident response plans should also be reviewed and updated as needed, including by making sure all emergency contacts are current. While there are additional cybersecurity risks that arise from working remotely, there are separate risks that arise from the need to respond to cybersecurity incidents when information security personnel are not located in the same place. Companies should engage an outside cybersecurity firm to provide incident response services and outside counsel, if they have not already done so, in order to be prepared and not lose critical time in the event that a cybersecurity incident occurs.
- ***Ensure Back-Ups*.** Companies should consider where crucial data resides, and ensure backups of the data exist and are secured separately from the company's network. The existence of these backups may be crucial in enabling the company to function in the event of a ransomware attack. Companies should also consider resiliency or redundancy measures if the communication channels they now rely on while operating remotely—like their videoconferencing vendor—are impaired.

* * *

ENDNOTES

1 World Health Organization, *Beware of criminals pretending to be WHO* (2020), https://www.who.int/about/communications/cyber-security.

2 Federal Bureau of Investigation, *FBI Sees Rise In Fraud Schemes Related To The Coronavirus (COVID-19) Pandemic* (Mar. 20, 2020), https://www.ic3.gov/media/2020/200320.aspx.

3 Caitlin Cimpanu, *Thousands of COVID-19 scam and malware sites are being created on a daily* Basis, ZD NET (Mar. 18, 2020, 15:47 GMT), https://www.zdnet.com/article/thousands-of-covid-19-scam-and-malware-sites-are-being-created-on-a-daily-basis/.

4 Cimpanu, *supra* note 3.

5 U.S. Dep't of Justice, *Lithuanian Man Pleads Guilty To Wire Fraud For Theft Of Over $100 Million In Fraudulent Business Email Compromise Scheme* (March 20, 2019), https://www.justice.gov/usao-sdny/pr/lithuanian-man-pleads-guilty-wire-fraud-theft-over-100-million-fraudulent-business.

6 Zack Whittaker, *Hackers are jumping on the COVID-19 pandemic to spread malware*, TECHCRUNCH (Mar. 12, 2020, 5:41 PM EDT), https://techcrunch.com/2020/03/12/hackers-coronavirus-malware/.

7 Federal Bureau of Investigation, *supra* note 2.

8 Cybersecurity and Infrastructure Security Agency, *Defending Against COVID-19 Cyber Scams* (Mar. 6, 2020), https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.

CONTACTS

New York		
H. Rodgin Cohen	+1-212-558-3534	cohenhr@sullcrom.com
Mitchell S. Eitel	+1-212-558-4960	eitelm@sullcrom.com
John Evangelakos	+1-212-558-4260	evangelakosj@sullcrom.com
Jared M. Fishman	+1-212-558-1689	fishmanj@sullcrom.com
Nicole Friedlander	+1-212-558-4332	friedlandern@sullcrom.com
Scott D. Miller	+1-212-558-3109	millersc@sullcrom.com
Matthew A. Schwartz	+1-212-558-4197	schwartzmatthew@sullcrom.com
Alexander J. Willscher	+1-212-558-4104	willschera@sullcrom.com
Michael M. Wiseman	+1-212-558-3846	wisemanm@sullcrom.com
Washington, D.C.		
Eric J. Kadel, Jr.	+1-202-956-7640	kadelej@sullcrom.com
Stephen H. Meyer	+1-202-956-7605	meyerst@sullcrom.com
Kamil R. Shields	+1 202-956-7040	shieldska@sullcrom.com
Jennifer L. Sutton	+1-202-956-7060	suttonj@sullcrom.com
Samuel R. Woodall III	+1-202-956-7584	woodalls@sullcrom.com
Los Angeles		
Anthony J. Lewis	+1-310-712-6615	lewisan@sullcrom.com
Robert A. Sacks	+1-310-712-6640	sacksr@sullcrom.com
Palo Alto		
Nader A. Mousavi	+1-650-461-5660	mousavin@sullcrom.com
Sarah P. Payne	+1-650-461-5669	paynesa@sullcrom.com