CAHILL

April 7, 2020

<u>COVID-19 and Cybersecurity for Remote Work</u>

COVID-19 has forced businesses to undertake an unprecedented shift towards remote work. With social distancing and quarantines becoming the new norm, cyber criminals already are taking advantage of these sudden and unexpected changes in behavior, and authorities have reported a predictable spike in COVID-19-related cyberattacks, particularly phishing emails, robocalls, and similar scams.[1]

As companies shift to working remotely, cyber criminals actively are refining their attacks. In this new environment, potential victims will face new and unexpected difficulties separating legitimate business requests from illegitimate scammers' tricks. For example, the increased use of personal devices and extensive remote access to company information systems heighten the vulnerability to hackers who may slip in a last-minute change to payment instructions that is purportedly explained by ongoing events and appears entirely authentic. The resulting losses can be as large as the amount of a corporation's largest wire transaction. To address these new risks and maintain business continuity, companies must reassess and reevaluate their cybersecurity operations. We outline below a variety of factors for companies to consider when doing so.

I. Cyber Leadership

A strong and consistent "tone at the top" focusing on the importance of data security and privacy is important. This regular messaging should remind employees that the organization takes these issues seriously. The appointment of a chief security officer, if not already designated, also can reinforce expectations that all employees must reliably and consistently follow all security protocols. If something does go wrong and regulators conduct a review, they will examine whether a company had designated such leadership and generally will look more favorably upon those who have.

II. Phishing

Even before the COVID-19 crisis, phishing emails stood out as the most significant security vulnerability for most victims. Now with most transactions originating and being performed remotely, the risk has been greatly magnified. Expanded employee awareness and training will be vital as new arrangements and accommodations are made. Effective and reliable authentication is both the challenge and the goal. Ensuring proper user access controls, such as multifactor authentication, is imperative. Many employees will be logging into work for the first time from private computers in their home that already may be compromised with malware. Weak controls and single factor authentication are ripe for exploitation during the COVID-19 crisis, and such breaches can linger undetected with catastrophic results.

Companies should encourage employees to communicate directly with colleagues and other relevant contacts – ideally by phone – to confirm any changes to plans, procedures, or other secure activities, especially those that are financial. Companies also should notify employees of the increases in anti-phishing activity and help them stay cognizant of risk factors and signs, such as social engineering tactics. Employees should be reminded regularly that if they see something, they should say something.

[1] *See FBI IC3, FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic, March 20,2020, available at* https://www.ic3.gov/media/2020/200320.aspx; *FTC Consumer Information, Scammers are taking advantage of fears surrounding the Coronavirus, available at* https://www.consumer.ftc.gov/features/coronavirus-scams-what-ftc-doing; and *U.S. Dep't of Homeland Sec. CISA, Defending Against COVID-18 Cyber Scams, March 6, 2020, available at* https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams.

III. Technical Challenges

The COVID-19 crisis has added new challenges on the technical side as well. Companies have been adding a multitude of new ways to work from home, all of which come with an assortment of new risks. First and foremost, companies should confirm that all new access points are secure and that technical defenses are fully implemented. To protect against ransomware attacks, backup data and timely restore functions should be fully operational and properly maintained. The ability to quickly restore hijacked systems from continuous backup remains the best way to make ransom demands irrelevant. Companies also should learn from past cybersecurity incidents, like the WannaCry ransomware attack,[2] and ensure that their patch management program is current and reliably updated.

IV. Incident Response

A security incident can ripple quickly across a business causing immense disruption. Therefore, it is vital to have a complete incident response plan and process in place that takes into account the current remote-working realities that we now face. In some jurisdictions, a security incident may necessitate a host of reporting obligations, including to customers and regulators. In addition, business contracts may include reporting obligations to vendors and insurers. Companies must be aware of these requirements. Further, an incident response plan should include processes denoting timely detection, appropriate assessment, and corrective action. Relatedly, companies should review their cyber insurance policies and their specific language to understand the scope of coverage, focusing on provisions related to force majeure, impossibility, and frustration. An incident response plan will ensure company leadership has a clear path forward, rather than addressing these critical matters for the first time while simultaneously dealing with the breach itself.

V. Remote Vendors

Companies should review vendor contracts, especially as they relate to any new vendor services necessary for employees to work remotely. Rushing the implementation of the remote access points can create new risks in an environment where employees are already under considerable pressure. For existing vendors, understanding contract terms will ensure vendors are meeting all security obligations without any deficiencies and with appropriate safeguards in place. Additionally, companies should map which vendors have access to valuable or sensitive data, as any issues with vendors that control or process data can multiply security gaps and ambiguity in covered responsibilities.

VI. Security Assessment

Finally, companies should conduct a security assessment to evaluate compliance in the new environment. Various regulations, including the European General Data Protection Regulation (GDPR),[3] already require companies to conduct security and privacy assessments, and regulators ask for such assessments when conducting

[2] In May of 2017, hackers demanding bitcoin ransom payments used WannaCry, ransomware with a worm component, to infect the Windows systems of organizations worldwide. Microsoft had released patch updates for the worm but affected organizations had failed to make the necessary updates.

[3] *See* EU General Data Protection Regulation (EU) 2016/679 of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2016 O.J. (L 119) 1 (Article 35 of the Regulation describes carrying out Data Protection Impact Assessments).

any review. If something goes wrong, they are likely to view the absence of a security assessment as a red flag indicating that the company was not focused on the problem. Using an outside consultant or law firm to conduct or review an assessment shows the opposite – both because of the perspective a professional third party can bring to the table and because it shows an organization is willing to commit resources and money to the problem. The use of outside counsel in directing the security assessment has the added advantage of enhancing privilege protections over the assessment process and findings.

In unpredictable times, preparation is imperative. To adapt to rapidly evolving business needs and combat bad actors taking advantage of current circumstances, companies should prioritize information security and reevaluate their IT systems. Data privacy laws and regulations may require certain companies to periodically assess their current architecture and demonstrate compliance, but all companies should take the opportunity to reevaluate their IT systems and consider engaging outside counsel for analysis.

*   *   *

If you have any questions about the issues addressed in this memorandum or if you would like a copy of any of the materials mentioned, please do not hesitate to call or email David Owen at 212-201-3955 or DOwen@Cahill.com; or Jason Yeoun at 212-701-3850 or JYeoun@Cahill.com; or email publications@cahill.com.