Skadden

Cybersecurity Challenges and Incident Response Preparedness During the Coronavirus Pandemic

March 25, 2020

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Daniel J. Scime
Associate / Chicago
312.407.0725
daniel.scime@skadden.com

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West
New York, NY 10001
212.735.3000

155 N. Wacker Drive
Chicago, Illinois 60606
312.407.0700

The spread of the novel coronavirus has upended Americans' lives in a matter of months. While life outside has ground to a standstill in many regions of the country, much of corporate America is meeting the unique challenges posed by the current epidemic by adopting remote working technologies and practices. Companies, determined to sustain growth and add value, are adapting long-standing business practices to enable telecommuting and empower a new cyber workforce. For their part, workers are relying to an unprecedented degree on digital tools to keep them connected to coworkers and to do their jobs while staying safe at home.

As record numbers of Americans have begun to log in remotely each day, many for the first time, the number of cyber vulnerabilities facing companies has also increased. Unfortunately, malicious actors have spotted the opportunity, increasing both the frequency and complexity of their attacks. Media reports from the past week noted a wave of attacks on remote access tools relied upon by companies whose workforces have been forced to stay home in the midst of the epidemic. Other reports indicate malicious actors have also begun disguising phishing emails as coronavirus updates from health authorities, leveraging familiar attack vectors while capitalizing on individuals' heightened fears regarding the pandemic.

Not only are well-known threats posed by phishing and ransomware exacerbated, but the unique cybersecurity challenges attendant to remote working in the current environment — the exponential growth of network access points, reliance on unsecured Wi-Fi networks and increased use of unpatched virtual private networks (VPNs) and devices — compound familiar cyber risks and increase the likelihood of a breach.

Much has been written about basic precautions that companies need to be taking to protect themselves from cyberattacks in the coming weeks and months. All companies should be working to develop and review systems, policies and procedures designed to secure their remote work spaces (*e.g.*, multifactor authentication, VPN/remote access system patching, enhanced system monitoring, firewalls). Executives should aim to increase employees' general awareness of IT support mechanisms in place to assist them while they work remotely and to alert them to specific anticipated issues, including, for example, the expected increase in phishing attempts and continued restrictions on the use of personal email and cloud storage services to conduct business. Also, management should test and, if necessary, increase the capacity of remote access solutions, and ensure that their business continuity plans are up-to-date.

© Skadden, Arps, Slate, Meagher & Flom LLP. All rights reserved.

Yet, beyond those precautions, companies must also consider how to ensure that IT security personnel are prepared to manage critical cybersecurity tasks — for example, log reviews, attack detection, and incident response and recovery — while working remotely. For many companies, cybersecurity management plans still assume physical access to servers and network access points, and even where physical access is not a technical requirement, teams may be reliant on their ability to quickly assemble in war rooms to coordinate a response to an incident.

Identifying and responding to an incident while key security personnel are themselves dispersed and working remotely will pose unique challenges, particularly in the current environment where local shelter-in-place orders and health concerns could prevent key team members from convening to coordinate a response or from accessing key infrastructure. In the worst cases, IT professionals responsible for identifying and containing breaches may themselves end up locked out of the remote systems they are charged with defending. Without physical access to affected servers and backup systems, protocols for responding to infiltrations may no longer be valid, and forensic analyses to determine the scope and severity of a breach could prove difficult or impossible. In all cases, however, remote response teams will, in the absence of adequate planning, face a multitude of potential logistical hurdles in coordinating an effective response.

With forethought, however, management and security professionals can plan for and mitigate these increased risks. Companies should:

- **Develop alternative communication channels.** Companies should establish alternative means of communication for critical response personnel to use when an incident occurs. In ordinary times, security team members can quickly convene in person in the office to coordinate a response if necessary. However, if an attack compromises email servers or web-based communication applications while security team members are working remotely, the company's ability to quickly coordinate an effective response could be compromised. It is therefore imperative that response teams have a well-documented and widely known plan that will enable them to quickly and effectively coordinate with each other to develop a response. Many companies' security teams already have dedicated, prearranged video and teleconference bridges and messaging platforms that allow them to quickly establish a remote war room. Companies that do not have these alternative communication channels in place should build them now; companies that do should test them to make sure they are working as intended.

  Companies must also prepare for the possibility that dial-in numbers and webexes will become overwhelmed or otherwise prove unreliable. Building redundancies into the response team's communication plan will help mitigate those risks. Similarly, those who rely on computer-based applications to store and retrieve relevant contact numbers and email addresses may lose that access if services are disrupted. Companies should therefore disseminate key team members' full contact information and develop old-fashioned phone trees that can be printed if necessary.

- **Plan for the possibility that key staff are unavailable.** Companies must also plan for the possibility that key security staff who would ordinarily handle incident response may be incapacitated or otherwise unavailable. At minimum, teams should be prepared to fill gaps if one or a handful of key personnel are sick, hospitalized or otherwise unavailable when an incident occurs. Companies may also want to consider having designated third-party security consultants in place to backfill as needed.

- **Review key response plans.** Companies should review key response plans with an eye toward identifying instances where staff members' physical presence onsite would ordinarily be required. Management should then develop a plan to either bypass the need for that physical presence or to ensure that necessary staff will be able to access critical infrastructure without compromising their safety or health.

- **Run tabletop exercises.** One common theme among companies that fall victim to devastating attacks is that despite investing in cybersecurity measures, they failed to execute their incident response plans. So-called tabletop exercises, which enable a company to work through a realistic security incident, can be invaluable for identifying latent issues in an incident response plan. In the context of a remote working environment, companies can leverage such exercises to identify key response processes that break down when employees are working in a distributed environment and communication is difficult.

- **Run VPN vulnerability scans.** Many companies are already required to run vulnerability scans by regulators like the New York Department of Financial Services. In the current environment, one focus of those scans should be the companies' VPN access points. Per the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency's (CISA) "Information and Updates on COVID-19," VPN vulnerabilities are at particular risk both because the "always on" nature of VPN access points means they are less likely to be up-to-date and fully patched and because hackers are therefore increasingly targeting them.

- **Balance the need for increased administrator privileges.** Companies eager to ensure robust incident response capabilities may be tempted to expand administrator privileges by broadening access rights or increasing the number of individuals who hold those rights. However, such rights expansions can be significant sources of vulnerabilities. Thus, companies should carefully weigh access needs for relevant logs against the increased risks and ensure that all privileged accounts are secured and monitored.
- **Review expert guidance.** A number of organizations, including CISA and the National Institute of Standards and Technology (NIST), have published expert guidance that companies can leverage to mitigate the risks of remote working and ensure that their IT security professionals are prepared to ramp up remote management of various key cybersecurity programs.

Some overseas regulators have expressed awareness of the extraordinary challenges facing corporations forced to urgently adopt dispersed work arrangements and arguably signaled their intent to be accommodating. For example, the U.K. regulator in charge of enforcing GDPR — the Information Commissioner's Office — recently said: "We understand that resources, whether they are finances or people, might be diverted away from usual compliance or information governance work. We won't penalise organisations that we know need to prioritise other areas or adapt their usual approach during this extraordinary period."

Still, companies should understand that all existing statutes and regulations establishing cybersecurity requirements, including data breach notification laws, remain in place. Additionally, HIPAA remains in force for companies handling confidential medical information.

For companies operating in the United States, meeting data breach notice requirements is a challenge in ordinary times given the various state statutes' short compliance windows. Delays stemming from the fact that key employees are working remotely and that vendors who often provide notice services may not be at full capacity underscore the need for companies to have well-rehearsed plans in place and react quickly to meet statutory obligations.

* * *

As companies transition to a remote workforce due to COVID-19, they are left exposed to new vulnerabilities that cyber attackers are poised to exploit. Now is the time for companies to reassess their incident response and business interruption plans to ensure they are ready for these new threats.