Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

COVID-19 Hacks Bring Cyber Hygiene Into Sharp Focus

By **Dorothy Atkins**

Law360 (April 14, 2020, 3:56 PM EDT) -- Companies are seeing a major uptick in the number of COVID-19-related cybersecurity attacks as employees shift to working remotely, prompting attorneys to urge clients across industries to ramp up security protocols for the long haul and be wary of adopting third-party software.

Since President Donald Trump declared a national emergency on March 13 to help combat the coronavirus outbreak, cybercriminals have been barraging health care, financial services and even law firms with phishing emails and ransomware attacks in an attempt to catch targets off-guard, according to a dozen cybersecurity attorneys who spoke to Law360.

The sophistication of the attacks are wide-ranging, and many of them attempt to lure in victims by offering information about COVID-19 and benefits under the recently passed Coronavirus Aid, Relief and Economic Security, or CARES, Act. In at least one recent attempted attack, cybercriminals aimed to steal a company's proprietary information and trade secrets, according to the attorneys.

Andrew Konia, chair of McGuireWoods LLP's data privacy and security team, said he's recently seen a number of phishing attempts that are designed to prey on the fear and anxieties surrounding the pandemic.

"We are seeing a lot of potential threats," he said. "It's depressing to see the environment taken advantage of like this, but of course hackers have no moral code and this is just a business opportunity for them."

Konia said that while some phishing emails are written in fragmented English and make nonsensical threats, others are more convincing, posing as real people and companies, making it more difficult to identify the email as a hoax.

"You don't think, you just click it," he said. "You just click, and those consequences can be devastating."

The rise in attempted cyberattacks have spurred clients to seek legal advice. David Kessler, Norton Rose Fulbright's head of data and information risk, said he's advised clients to be diligent in practicing good cyber hygiene.

Kessler said hackers take advantage of targets during times of crisis and when they otherwise might have their guard down, such as during holidays and over weekends.

“There’s a reason I get most of my calls Saturday morning, because they attack Friday night,” Kessler said.

To make matters worse, Kessler said, there is also less IT staff working, and those that are working are working remotely.

Yet experts who spoke to Law360 detailed a host of steps companies can take to help avoid and mitigate breaches from COVID-19-related cyberattacks.

Tighten Security With VPNs and Multifactor Authentication

Kessler tells clients that they should be using multifactor authentication to access corporate devices and networks, only giving employees access to internal systems if they need it. That way, he said, if an employee’s account is compromised, it doesn’t expose the rest of the business’ infrastructure.

“An ounce of prevention is worth 20 pounds of cure,” Kessler said.

Faegre Drinker Biddle & Reath LLP partner Ken Dort said he recommends that remote workers use virtual private networks, or VPNs, to secure their networks, and that VPNs be regularly updated. However, he emphasized that companies can’t rely solely on VPNs for protection.

Train Workers to Spot an Attack

Dort stressed the importance of employee training, noting that workers need to know how to properly activate VPNs and be on guard against phishing attempts and suspicious links. They also should know what to do if they expose a network to a breach, and there should be IT staff on hand to respond quickly, he said.

Lisa Ropple, leader of Jones Day’s cybersecurity, privacy and data protection practice, agreed that VPNs alone will not protect against all attacks. As VPNs have become more popular, she said, hackers have targeted their efforts in trying to exploit their vulnerabilities.

“Certainly VPNs were never intended to be used on the massive scale that they are now,” she said.

Ropple also said employers should specifically warn employees that a phishing attempt could come in a COVID-19-related email and that companies should implement specific protocols — which aren’t shared over email — to prevent fraudulent money transfers from being processed.

Avoid Data Sprawl

Andreas Kaltsounis, co-leader of BakerHostetler’s national digital risk advisory and cybersecurity team, said part of the challenge with securing a remote business is that a cybercriminal’s “attack surface” becomes significantly larger and difficult to protect.

Kaltsounis explained that workers and managers might use their own personal devices, software, video-conferencing tools or file-sharing services just to get the job done, which can allow for inadvertent data sharing and unsecured data sprawled across various platforms.

“Attackers can take advantage of those things happening,” he said, adding that’s why it’s important for employers to provide workers with the resources and tools they need. He said it’s important that companies implement changes with the mindset that they will be in place over the long term and are not quick “knee-jerk” fixes.

“We all recognize that the data protection [and] cybersecurity issues around the crisis may not be the primary concern — and shouldn’t be the primary concern,” Kaltsounis said. “Frankly, just keeping the business running is what organizations are primarily focusing on. But it does no good to get the workforce working from home if the way you do it is going to invite a ransomware attack that entirely cripples the business later.”

Latham & Watkins LLP partner Jennifer Archie also noted that most companies have now had weeks to shift to remote work, so their IT efforts should be ramped up to ensure they’re protecting against potential cyberthreats.

“As weeks go by, it becomes harder to say you didn’t have time to adapt,” Archie said. “COVID-19 is not a very durable excuse. It’s going to time out at some point as we go through this.”

Vet Third-Party Vendors

As more companies work remotely, Dominique Shelton Leipzig, the co-chair of Perkins Coie LLP’s ad tech privacy and data management practice, said it’s also important to vet third-party vendors that provide businesses with critical software.

“It’s very important to have conversations about cybersecurity before bringing that vendor on board,” she said.

Leipzig added that the vetting process doesn’t have to take weeks to complete, and it can be quicker if vendors are certified under the Center for Internet Security’s Critical Security Controls.

“We are really in unprecedented times, and it’s going to call for unprecedented rigor that companies have already put in place,” she said.

Protect Video Conferences With Passcodes

To address potential video-conferencing vulnerabilities, Crowell & Moring LLP's Jeffrey Poston, co-chair of the firm's privacy and cybersecurity group, is advising clients to follow recommendations from the FBI, which published a letter earlier this month in response to so-called "**Zoom-bombing" attacks,** or when hackers pop into and disrupt meetings on the video-conferencing service.

The letter encourages users to ensure meetings are private, either by requiring a password or controlling guest access from a waiting room, or to choose a service provider that offers end-to-end encryption.

Other attorneys are advising clients to limit what they discuss and display on video calls, or have a staff member monitor the calls for suspicious activity.

Jena Valdetero, co-leader of the data privacy group at Bryan Cave Leighton Paisner LLP, advises clients to be wary of any video-conferencing tool that is free, because they tend to be less secure and often make money by selling information such as the type of call being made.

She added that even if a company purchases a service, clients should still read the product's privacy policy to ensure they're not exposing themselves to additional vulnerabilities.

Create an Incident Response Plan

Valdetero also noted that companies should have printed hard copies of their incident response plans to ensure everybody knows what to do if a business' computer network is compromised.

Additionally, she said management should have a list of contacts to reach out to in responding to such an attack, including insurers, outside legal counsel that specialize in data breaches, and one or two forensic investigators.

Ropple added that some insurance policies that cover cyber loss claims include a provision that requires policyholders to notify insurers of a breach within a certain time frame.

"Companies should be familiar with their policies and know who to notify," she said.

O'Melveny & Myers LLP special counsel Scott Pink said he's also fielded questions from clients about privacy issues related to collecting employee health information. He said he's advised them that they should not overlook privacy laws and regulations in responding to requests for information from the government about worker health, because regulators have indicated they will enforce privacy statutes.

"It's a little bit on the fly, but these companies need to do the best they can do to comply," Pink said.

--Editing by Philip Shea and Alanna Weissman.
