COVID-19 POSES INCREASED CYBERSECURITY RISKS TO EMPLOYERS AND BUSINESSES

by Caleb Green and Sara Jodka

Evolving developments and news surrounding COVID-19 (the "coronavirus") has prompted immediate action from employers and businesses worldwide. While many businesses have been forced to temporarily shut down, the ones that remain operational have been forced to adjust to working remotely and adopt other protocols to ensure the health and safety of their employees and customers. As employers face the challenge of balancing business with growing health concerns related to the coronavirus, they face additional challenges as their cybersecurity protocols will be tested like never before.

Cybercriminals love a good crisis and uncertainty to manipulate and exploit individuals through cyber-threats, and they also use newly-implemented technologies to try to penetrate a business's systems. As businesses implement safety strategies in response to the coronavirus pandemic, they must prioritize data protection and cybersecurity concerns to limit their exposure and legal liability.

Specifically, employees working remotely can create risks to businesses in the following ways: (1) increased risks from remote access, including physical security risks associated with use of company-owned and personal devices; (2) increased phishing and other scams; and (3) violation of industry- and state-specific laws.

INCREASED RISKS FROM REMOTE ACCESS

In response to the widespread transmission of the coronavirus, many employers are providing employees with remote access options, enabling them to work outside of the corporate infrastructure. While providing a work-from-home option for employees may be a prudent measure to prevent the spread of diseases throughout the workplace, corporate leaders should be wary that remote systems can expose businesses to cybersecurity risks. Remote access relies on the exchange and transmission of information and data, typically over the Internet. While teleworking, employees may be handling, accessing, discussing, or transmitting sensitive information, including company trade secrets, customer personal information, or confidential financial data.

Since this pandemic started, there has been a palpable uptick in business email and other interruptions, including where Office 365 or Gmail accounts were hacked through phishing scams. One particularly effective scam has been when the hacker sends a fraudulent invoice purporting to be from a legitimate worker with changed wiring instructions where the money transferred goes to the hacker's account. By the time a company reconciles its accounts receivables and realizes what has happened, the money is gone and there is usually no way to recover it. Further, the businesses have paid for goods/services they did not receive, and the account is still due because the money was paid to a criminal element. For this reason, it is good cybersecurity hygiene to enable multi-factor authentication on accounts the business controls, train employees on these types of schemes, and require they speak directly to a person before they change any ACH/direct deposit or other information.

Another issue in a work-from-home environment is where employees use employer-issued or personal devices to access corporate data. Namely, employers risk physical loss or theft of sensitive information stored on corporate devices when they permit employees to access the systems remotely. Furthermore, an employee's remote access in a public setting, such as a coffee shop or their private home network, can expose sensitive information through eavesdropping, networking hacking, and other forms of unauthorized access. For this type of scheme, hackers try to manipulate the network by mimicking the name of the secure network so employees trying to connect think they are connecting to a legitimate network when they are not. For example, when working in a hotel, a common public designation is "Ballroom," "Conference Room," and similar. To get to the top of a user's WiFi choices, hackers will use "Ballroom 1," "Conference Room 1," etc. To ensure safety, businesses should require employees to only work on secure, password-protected internet connection and when using public WiFi, if that is the only option, users should check with the facility to ensure they know what WiFi networks are legitimate so they can easily determine which ones are not.

Another budding issue with the increased workforce is the use of teleconference apps. Zoom and other video-conferencing functions and applications have gained significant popularity among the remote workforce, but there are a number of concerning privacy issues included in Zoom's Privacy Policy, which was modified on March 29, 2020, and some of the more concerning privacy features were deleted. For example, Zoom can:

- Share data with third-party advertisers, including videos, messages, documents, contact information, etc.;
- Use video content for targeted advertising campaigns;
- Zoom hosts may record and share the session with others, but this puts the onus on the host to obtain consent for those in all-party consent states, though consent would not be necessary in one-party consent states; and
- Zoom hosts can also activate "Attention Tracking" to see whether individuals click away from the Zoom meeting for more than 30 seconds.

Zoom is not alone in their privacy practices as all video-conferencing platforms have similar policies. That being said, it is important to fully understand the scope of these policies, especially when using these platforms to conduct medical/healthcare appointments or to conference with minors. Many of these platforms are not HIPAA-compliant, nor are they pretending to be, so ensure that when transmitting HIPAA-protected information that all transmissions are done through a HIPAA-compliant telehealth platform. In fact, the Office of Civil Rights and the Department of Health and Human Services, which is the government agency that enforces HIPAA, has issued guidance on telehealth remote communications and issue issued 11 FAQs on Telehealth and HIPAA during the COVID-19 nationwide public health emergency.

Another issue for remote workers, and their employers, is that even from the comfort and convenience of their own homes, employees can expose sensitive corporate information via voice assistance systems, smart speakers, and home surveillance systems such as Siri, Google Assistant, Amazon Alexa, Echo, and Ring. All of which have grown in popularity within households in recent years, but remain vulnerable to many forms of hacking. In fact, these systems have a history of security vulnerabilities that have led to eavesdropping and spying. Namely, hackers have targeted Ring—a home security company owned by Amazon—by hacking user accounts and gaining access to cameras and microphone hardware embedded within the home security system. In recent events, hackers were able to access Ring cameras within the home, spy on the homeowners and their family members, and even communicate with them using the microphone feature.

Smart speakers, virtual assistants, and smartphones also pose a significant risk to the unaware teleworker. Researchers and white hackers have exposed vulnerabilities in smart devices such as Alexa Echo, Siri, and Google Assistant. Cybercriminals can use nearly silent ultrasound waves to trigger these smart devices to prompt users for their user credentials and passwords as well as force the devices to executive malicious commands. Given the increased number of employees working from home amid the COVID-19 outbreak, hackers will likely continue their attempt to thwart these technologies and systems founds within and throughout the home.

PHISHING ATTACKS

The leading cause of cyber-attacks worldwide is phishing attacks. Phishing is the use of electronic communications, including phone calls, text messages, and even social media tools, to disguise fraudulent communications as legitimate messages from trusted sources. Through these attacks, hackers seek to acquire sensitive information and often will contain malware-infected attachments or a link that, if opened, will install malicious software on the device and surrender sensitive information. Cyber-attackers couple social engineering schemes with phishing ploys to manipulate employees and customers to carry out specific tasks, such as opening the malware-infected attachment, clicking the compromised link, or otherwise divulging confidential information. In light of the widespread transmission of the coronavirus, these cyber risks are compounded as cybercriminals are using the fear and uncertainty surrounding this international emergency to further manipulate employees through phishing schemes. For example, the U.S. Department of Homeland Security reports that to gain access to valuable corporate information, cybercriminals are sending phishing emails posing to be trusted health organizations including malware-infected attachments purporting to contain important information regarding the coronavirus.

The Internet is inundated with phishing schemes that are piggybacking off the COVID-19 pandemic. In February 2020, cybercriminals released a website purporting to be a distribution map of the coronavirus outbreak. The malicious online map, which was located at www.coroa-virus-map[.]com, hosted a convincing impersonation of the legitimate map operated by the John Hopkins Center for Systems, Science and Engineering and offered what appeared to be a tally of the confirmed cases and deaths related to the virus outbreak. However, unbeknownst to users that navigated to this site, malicious password-stealing software was being installed on their computers and mobile devices.

Another COVID-19 related phishing attack mimicked an official email correspondence from the World Health Organization (WHO). The email, which carried the WHO logo, contained a link to a document purporting to contain information regarding preventing the spread of the virus. Instead, the link redirected victims to a malicious website, which attempted to harvest sensitive credentials, including passwords and usernames.

Through these deceiving mechanisms, cybercriminals are actively taking advantage of employees and customers as they attempt to navigate the confusion and barriers resulting from the coronavirus pandemic. As a result, businesses are at increased risk of losing valuable intellectual property, sensitive data, and financial information.

INDUSTRY AND STATE-SPECIFIC LAW COMPLIANCE – STATE DATA BREACH NOTIFICATION REQUIREMENTS, GDPR, CCPA, GLBA, AND HIPAA

While touched on briefly above in regards to HIPAA, remote work can also trigger industry- and state-specific law compliance issues. While remote working is somewhat novel, these state- and industry-specific laws are not. The same standard rules and requirements apply. Further, with so many events being canceled or pushed back, many assumed the effective enforcement date of the California Consumer Privacy Act (CCPA) of July 1, 2020 would be postponed. It will not, and July 1, 2020 remains the anticipated date by which the California Attorney General will begin to enforce the CCPA.

CYBERSECURITY TAKEAWAYS

As employers and businesses implement safety and health measures to combat the spread of coronavirus, corporate leadership should consider the following additional corporation actions and best practices:

1. Consult with an information security professional or service provider to ensure your organization is properly equipped with the proper technology (e.g. firewalls) and safeguards to reduce the risk of cybersecurity breaches.
2. Establish a Telework Security Policy that defines which permissible forms of remote access, which types of telework devices are permitted to use each form of remote access, and the type and amount of access each type of teleworker is granted, and identify and specify particular information and documents that require the utmost care in its handling.
3. Specify in writing what employees can and cannot do in the handling of sensitive/protected information.
4. Require any PI and PHI be encrypted before being transmitted.
5. Ask employees to specify which devices they will use for work and provide encryption services with a company certified security software.
6. Equip employee devices with remote access capability, security software, and the latest manufacturer software updates.
7. Ask employees to password-protect their personal networks with WPA2 encryption.
8. Equip employee issued remote access devices with access controls that limit employee access to minimum services and functions, including disabling employee's use of administrative privileges use of external thumb drives, hard drives, and third-party cloud services (e.g. Google Drive, DropBox).
9. Require employees to return sensitive files and paper documents to the office or corporate infrastructure, especially financial and healthcare-related documents
10. Require multifactor, two-step authentication for employee remote access.
11. Require employees to periodically change their username and password credentials.
12. Require employees to use an encrypted virtual private network (VPN) for remote access.
13. Include warning labels on incoming messages and emails that originate from outside of the corporate infrastructure.
14. Advise teleworkers to refrain from using a speakerphone or conducting work-related conversations in the presence of smart speakers or home surveillance (e.g. Alexa Echo, Google Home, Siri, Ring).
15. Opt-out of cookies each time when using video-conference apps/functions.

ABOUT THE AUTHORS

Sara H. Jodka is a Member of Dickinson Wright's Columbus office. She can be reached at 614.744.2943 or sjodka@dickinsonwright.com.

Caleb L. Green is an Associate in Dickinson Wright's Las Vegas office. He can be reached at 702.550.4417 or cgreen@dickinsonwright.com.