CBA Report

Cincinnati Bar Association

May/June 2020

2020-2021 CBA President Christopher A. Wagner

Feature Article

Managing & Mitigating the Increased Cybersecurity Threats Posed by COVID-19

By David J. Oberly

In recent weeks, the novel coronavirus (COVID-19) has taken the United States by storm, impacting companies from coast to coast in myriad ways and causing unprecedented changes in daily business operations. Cyber criminals are acutely aware of these seismic shifts and are engaging concerted campaigns to exploit these vulnerabilities which, in turn, has created noteworthy cybersecurity and data security risks and threats for organizations of all types. In particular, phishing and other types of cyberattacks have increased exponentially during the current public health crisis, as malicious actors seek to take advantage of the increased anxiety and elevated desire for information and resources regarding the pandemic. The rapid move to remote working has also created a vastly expanded attack surface for cyber criminals to exploit, as well as its own set of unique and heightened organizational cybersecurity and data security challenges. Companies must effectively guard against these imposing threats and be prepared to take immediate action in the event they become a victim of a successful cyberattack or other data compromise event.

Cyberattacks on the Rise: Coronavirus-Themed Phishing Scams & Hacking Campaigns

The public health crisis caused by COVID-19 has created a perfect storm for cybercriminals, who have found an opportunity to cash in on the fear and panic gripping the country by targeting companies and their workers with sophisticated phishing scams and other cyberattacks.

Hackers are deploying these cyberattacks in a range of different ways, both through email and websites. One common technique is to disguise emails directed to employees as originating from their employers or high-level management, with "updates" on company contingency plans and travel restrictions. Here, cyber criminals utilize social engineering to target employees with malicious messages, hoping they are even more susceptible than normal and will quickly click on a link (or otherwise take action) in response to urgent alerts from "management" requesting immediate action on a coronavirus-related issue.

Cyber criminals are also leveraging the emergency as cover to spread malicious activity. While cyber criminals often tailor phishing scams to seasonal events, such as tax season W-2 scams, the success rate of these traditional phishing scams is dwarfed by those tied to critical world events, such as this. In one scam, hackers target unsuspecting recipients with emails purportedly originating from a virologist, which contain malicious links and attachments that claim to provide information on how to prevent the spread of the disease. **Over 16,000 coronavirus-related Internet domains have been registered globally since January 2020**, and are **50% more likely to be malicious** as compared to other domains registered during that time period.

Additional Cyber Risks and Threats Arising From Remote Working

To further complicate matters, the rapid community spread of COVID-19 has swiftly pushed employees out of brick-and-mortar buildings and into home offices, as companies across all industries hurriedly turn to remote working arrangements, both as a precautionary measure and as a response to stay-at-home orders issued by many states. Cyber criminals are also seeking to exploit these operational changes by taking advantage of the often-inadequate security postures and other unique vulnerabilities of remote working.

Remote working increases company cyber and security risks and threats in several ways. First, it significantly enhances the likelihood that cyber criminals' targeted phishing campaigns and other attacks will be successful, as the vulnerable remote workers being targeted are both prone to becoming distracted at home, and also frequently mix personal online activity with their work-related endeavors. Many employees are generally inexperienced with remote working, and fail to practice safe computing practices while working outside of the office. These include the use of unsecured internet connections, especially public Wi-Fi, which can leave workers' remote devices susceptible to cyber attacks. Physical security is also a significant risk, as some employees will inevitably misplace or lose their mobile devices, allowing them to fall directly into the hands of malicious actors.

Compliance Tips

To protect against the elevated cyber and security risks that exist today in connection with the ongoing COVID-19 public health crisis, companies should consider the following best practices:

- **Cybersecurity & Data Security Policies:** First, companies should ensure they have cybersecurity and data security policies in place that directly address the use of organizational technology and remote working. To protect against phishing attacks, companies should maintain a corporate communications policy, which sets forth detailed guidelines on how the company will communicate securely with other members of the organization. **To guard against the increased risks stemming from remote work, important policies include systems access, physical access, acceptable use, removable media, mobile device/bring-your-own-device ("BYOD"), internet use, email use, and wireless communication policies.** Companies must ensure these policies are clearly communicated to all employees and are readily accessible to all members of the organization.

- **Incident Response/Disaster Recovery Plans:** With the increased security risk of phishing attacks and remote working, companies should maintain incident response and disaster recovery plans that can be implemented immediately with adequate resources to respond to a data breach or other cyber incident. These plans should be reviewed with key personnel to ensure everyone is up to speed on their roles and responsibilities in the event the plan needs to be put into action. It is also important to know how to contact key personnel and members of the incident response team if they are not working on-site or if normal communications channels are not available.

- **Employee Education:** Companies should ensure workers are thoroughly educated on the significant threats posed by coronavirus-themed cyber attacks and remote working, and how to effectively minimize those threats. Employees must be cautioned not to provide any sensitive company or personal data through email, and to be on high alert for coronavirus-themed cyber fraud. Employees must also be educated on how to spot attempted phishing attacks and best practices to follow to avoid the poten-

LCNB
National Bank
Discover the Difference
LCNB National Bank's Trust Department provides investment, wealth planning, and professional estate and trust services.
513-677-2203 | LCNB.com
FDIC
Our experienced trust professionals are highly accessible and are committed to timely, face-to-face meetings.
NOT FDIC Insured
No LCNB National Bank Guarantee
May Lose Value

tial pitfalls of phishing scenarios. Key tips for employees include being suspicious of emails with generic greetings and improper grammar style; never clicking on a link without first verifying the link destination by hovering the cursor over the URL; and never transmitting sensitive personal or company information via email. Companies must impress upon their workforces the importance of proper data security habits, and fully educate employees on how to safely and securely use, transfer, and store sensitive company data while working remotely.

- **Virtual Private Networks:** Virtual private networks (VPN) are a key piece of technology that add an extra layer of security by creating a safe, encrypted connection—a private network—from less-secure public internet connections. Companies with VPNs in place should ensure employees access company networks, systems, and data remotely by using the VPN whenever possible.

- **Password Practices:** Companies should require multifactor password authentication for access to all remote devices. This is critical to limiting potential damage when credentials or devices themselves are lost or stolen. In addition, all "remember my password" functions should be disabled on devices and applications that allow employees to access company networks and systems remotely.

- **Mobile Device Management:** Companies should consider utilizing mobile device management (MDM) software to increase the level of security on employees' mobile devices. MDM tools allow companies to monitor, manage, and secure employees' devices that hold company data and provide the vital ability to remotely activate a range of security measures, including data wiping on lost or stolen devices.

- **User Access Restrictions and Control:** Companies should consider restricting access to sensitive data by remote workers and adhering to the **principle of least privilege**, in which employees are granted only the minimal level of access or privilege that is necessary for them to carry out their duties. By ensuring employees only have access to data essential to their jobs, companies can significantly limit the scope of their potential attack surface. In turn, this can significantly decrease the likelihood that they will experience a data breach or other cyber incident.

- **Public Wi-Fi Bans:** Public Wi-Fi networks are one of the most common attack vectors for cyber criminals due to their lack of security, which makes it extremely easy to intercept credentials and data over these networks. As such, companies should strongly consider banning employees from accessing their networks, systems, and data through public Wi-Fi.

Conclusion

The COVID-19 public health crisis has caused unprecedented disruption in the operations of businesses across all industries and in all parts of the country. Cyber criminals are aware of this period of extreme uncertainty and rapid change, and are actively seeking to leverage and exploit the vulnerabilities that arise as companies respond and adapt to new remote working challenges.

Consequently, vigilance and strict adherence to strong cybersecurity and data security practices and habits are an absolute necessity to ensure that companies avoid finding themselves on the receiving end of a potentially catastrophic coronavirus-themed phishing attack or other type of cyber campaign stemming from remote working arrangements.

Those entities that have yet to put in place the necessary policies and practices to effectively defend against today's outsized cyber and security threats should immediately consult experienced legal counsel to ensure they implement proper safeguards to protect the security of all organizational networks, systems, and data during this period of increased vulnerability and risk. And in the event a successful cyber-attack does take place, companies should promptly consult and retain legal counsel to assist with managing the company's response, which will require taking immediate action to minimize the fallout of the event.

David J. Oberly is an attorney in the Cincinnati office of Blank Rome LLP and is a member of the firm's Cybersecurity & Data Privacy and Privacy Class Action Defense groups. David's practice encompasses both counseling and advising sophisticated clients on a wide range of cybersecurity, data privacy, and biometric privacy matters, as well as representing clients in the defense of privacy and biometric privacy class action litigation. He can be reached at doberly@blankrome.com. You can also follow David on Twitter at @DavidJOberly.