March 6, 2020

Mitigating Cybersecurity Risks Related to the Coronavirus

The outbreak and continued spread of a new strain of coronavirus, COVID-19, present unique challenges for companies. To protect employees and limit the spread of the virus, many companies have been implementing contingency plans that allow or, in some cases, mandate that certain employees work remotely. These efforts may be prudent and advisable, but can inadvertently heighten the risk of data breaches or other cyber incidents, which in turn can lead to substantial financial loss, reputational harm, and legal exposure. Although those risks cannot be eliminated, businesses should be mindful of the enhanced risks and consider reasonable, practical steps to mitigate them.

Heightened Risks

A spike in the number of employees working remotely can create increased network vulnerability, greater risk of inadvertent data loss, and greater financial vulnerability. These risks are exacerbated by cybercriminals seeking to exploit the unique features of the coronavirus situation to engage in more effective phishing and other methods to gain unauthorized access to network systems.

Network Vulnerability Resulting from Increased Use of Remote Access

Although methods of remote access vary across institutions, allowing employees to access the network remotely can create greater vulnerabilities, particularly for those institutions that quickly put in place or expand the use of remote access as in response to a situation like the coronavirus outbreak. When employees use unsecured home networks, for example, or, even worse, public networks such as those at coffee shops, communications may be vulnerable to eavesdropping and man-in-the-middle (MITM) attacks. In addition, some remote access endpoints only require a simple ID and password to log on, which may be susceptible to hacking given the frequent use of weak passwords. And, the use of BYOD devices raises additional concerns. If a device is used on external networks, infected with malware, and then connected to the company's network, the malware may spread across the network. Moreover, BYOD devices generally are more vulnerable to malware since they often are protected by weaker passwords and consumer-ready antivirus products that are not designed to fend off more sophisticated hacking techniques.

Companies that regularly use these remote access methods generally have policies and protections in place and have trained employees who use these technologies. But companies that are quickly implementing remote access in response to the coronavirus outbreak, or expanding access to greater numbers of employees, may not have had time to put in place such measures. In addition, for companies that have historically limited the use of remote access, the sudden increase in remote access activity on their networks may make it more difficult to monitor, detect, and prevent unauthorized activity.

Risk of Data Loss Resulting From Removing Data from the Office

An increase in employees working remotely also means that employees are more likely to take electronic or other data outside the physical, secure boundaries of the office space, or turn to shortcuts that may be more convenient but less secure, such as forwarding emails or documents to their personal email accounts. All of these can increase the risk of data loss, a particular concern for companies and employees with access to personally identifiable information or other sensitive customer or business information. Laptops or other devices are more likely to be lost or stolen when removed from the office, and, depending on the level of encryption (if any), the data on a stolen or lost device may be accessible to unauthorized users who come into possession of the device. And, employees may use thumb drives or other portable media to remove files from the office to make them accessible at home. Use of such portable media enhances the risk of accidental loss or theft. Moreover, if an employee is using portable media on a personal device at home, and then plugs that portable media into a work computer when he or she returns to the office, there is a risk of infecting the broader network.

Risk of Financial Loss Due to Feasibility of Controls

Employees who are not in the office are also not available to meet in person, and may not be able to answer their office telephones. As a result, companies that rely on personal contact, or telephone confirmations, to execute banking or securities transactions may be especially vulnerable to bad actors impersonating employees, or to employees circumventing security precautions because they are inconvenient or impossible to follow. For example, last year a financial institution was fined for failing to follow its own procedures that required the institution to call a customer to verify a wire transfer that turned out to be fraudulent.[1] When employees are working at home, it may become difficult or impossible to reliably reach them by phone, or to meet with them in person to verify or confirm transactions or instructions.

Increased Scams and Phishing Attempts Making Use of the Coronavirus Outbreak

Unsurprisingly, cybercriminals are taking advantage of the public anxiety and disruption to ordinary routines resulting from the coronavirus. Since January, bad actors reportedly have been sending an increasing number of phishing emails mentioning the coronavirus, posing as business partners or public institutions to lure recipients to open the messages, thereby unleashing malware. Some emails are made to look like a company's purchase order for face masks, to trick employees into wiring payments to fraudulent accounts. Others purport to provide updated health information on behalf of a public health organization, or promise information about a company's remote-work plan in exchange for personal details. In the midst of increasing disruption to normal work routines, cybercriminals can use the anxiety and urgency around the coronavirus to execute more effective spoofing and spear phishing attacks that trick users into taking actions that permit the bad actors to gain access to a company's systems.

Practical Steps to Limit Risk

There is, of course, no way to eliminate the risk of a data breach or other cyber incident. And, it can be especially challenging to limit those risks in the face of a rapidly changing and unpredictable public health situation such as this, where institutions must be able to react quickly. But because of the potential consequences of a cyber incident, companies must be especially vigilant and mindful of the increased risks. We set forth below some practical steps to consider in mitigating those risks.

1. Management (and, where appropriate, the board) should consider consulting with IT security professionals regarding cybersecurity risks presented by increased remote work and/or changes to standard protocols, and explore potential enhancements to existing security measures.

2. Antivirus and monitoring tools should be updated regularly, and companies may wish to consider endpoint detection and response software to remotely limit the impact of a compromised device.

3. Employees working remotely should be advised and/or reminded of relevant policies and restrictions.

4. If possible, employees should be asked to test the relevant remote access software and applications in advance to ensure that they are familiar with the process and allow time to address any problems or concerns.

5. All employees should be reminded of best practices, warned about the increased risk of scams and phishing attempts, and encouraged to be vigilant, including by avoiding links or attachments from unknown or suspicious sources. Some companies may even want to consider a simulated spear-phishing campaign to test its employees' awareness.

6. Companies that rely on policies and protocols that require in-person or telephonic confirmation of financial transactions should consider the challenges posed by the current health situation and whether enhanced protocols may be warranted to mitigate the risk posed by bad actors.

7. Companies should review, evaluate, and update, if necessary, their incident response and business continuity plans. Among other things, it may be important to ensure that if large segments of the workforce are working remotely, the necessary personnel, including IT and IT security, senior management, external advisors, and other relevant professionals, are accessible and can be contacted quickly even if not physically present in the office. This personnel includes not only those with the technical expertise to assist with a cyber incident, but also members of management with the appropriate decision-making authority.

8. Public filers should consider disclosure requirements concerning cybersecurity risks,[2] and in the event of a cyber incident, all companies should evaluate potential disclosure obligations, including to customers, government agencies, and, if applicable, investors.

Some of the steps companies are taking to mitigate the health risks associated with COVID-19, while prudent and responsible, may also increase the risks of a cyberattack, and companies should therefore also be considering reasonable and practical steps to limit those risks as well.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

H. Christopher Boehning
+1-212-373-3061
cboehning@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Jeh Charles Johnson
+1-212-373-3093
jjohnson@paulweiss.com

Brad S. Karp
+1-212-373-3316
bkarp@paulweiss.com

Loretta E. Lynch
+1-212-373-3000

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Richard C. Tarlowe
+1-212-373-3035
rtarlowe@paulweiss.com

Counsel Steven C. Herzog and Law Clerk Simona Shimeng Xu contributed to this Client Memorandum.

---

1 *See* Paul, Weiss, *CFTC Fines Phillip Capital for Failure to Prevent a Cyber Attach That Resulted in the Theft of Customer Funds* (Sept. 23, 2019), https://www.paulweiss.com/media/3978895/23sep19-cftc-phillip.pdf.

2 *See* Paul, Weiss, *SEC Reporting Companies: Considering the Impact of the Coronavirus on Public Disclosure and Other Obligations* (Mar. 4, 2020), https://www.paulweiss.com/media/3979380/4mar20-covid-19-update.pdf.