Employee Relations
LAW JOURNAL

Managing Security Risk: How COVID-19 Pandemic and Work-from-Home Arrangements Pose New Security Considerations

Meighan E. O'Reardon and Mia Rendar

The authors review a number of cyber risk factors arising from work-from-home arrangements as employers continue to navigate the COVID-19 crisis.

As if a global pandemic was not enough to trigger hypervigilance, cybercriminals have seized the COVID-19 crisis as an opportunity to exploit individuals' and organizations' cybersecurity vulnerabilities.

The Federal Bureau of Investigation ("FBI") anticipates[1] a rise in cyber-exploitation during this time, and has warned citizens of the various means of launching a cyberattack. In recent months, amid the precautions and stay-at-home orders to curb the spread of COVID-19, the global workforce has changed drastically to work-from-home environments. This shift poses its own unique risks to both personal cybersecurity, and that of third-party service providers. What's more, cyber actors are capitalizing on panic and uncertainty by using insidious means to gain access to the personal information of businesses and individuals. Your organization should consider some of the following cyber risk factors as we continue to navigate this unprecedented COVID-19 crisis.

Meighan E. O'Reardon, a partner in Pillsbury Winthrop Shaw Pittman LLP, focuses her practice on negotiating and managing complex services transactions across multiple industries, most notably in the financial services and healthcare sectors. Mia Rendar is an associate in the firm's Global Sourcing & Technology Transactions practice. Resident in the firm's office in Washington, D.C., the authors may be contacted at *meighan.oreardon@pillsburylaw.com* and *mia.rendar@pillsburylaw.com*, respectively.

AVOIDING SUPPLY CHAIN OR THIRD-PARTY NETWORK RISKS

While latter portions of this article discuss individual actions that can be taken to avoid cybersecurity risks during the COVID-19 crisis, safe networks start with the right enterprise-level infrastructure. Part of that infrastructure is the operational and contractual measures to respond to, and hopefully contain the effects of, a data security incident involving an outsourced service provider. The right contractual obligations put in place with third-party suppliers before a cybersecurity breach occurs can mitigate the occurrence of an incident and manage risks in the wake of one.

RESPONSIBLE AND PROACTIVE CONTRACTING

Whether an organization is contracting for technology to specifically assist the new work-from-home environment, like virtual meeting applications or cloud service providers, or if the organization is simply entering into a services contract for business-as-usual, now is the time to further clarify cybersecurity requirements during the contracting process. Many contracting documents and policies were likely drafted in a pre-COVID-19 environment, where the labor force was not predominantly on their home systems or utilizing alternative technologies.

Agreements with service providers should include robust security provisions that account for the sensitivity of the customer's data being handled in these alternative settings, and the documentation should clearly outline the rights of the customer and obligations of the service provider in the event of an information security breach. While audit provisions and other physical controls are a critical component of ensuring that a supplier's cybersecurity practices are aligned with contractual obligations, those same provisions are not necessarily drafted to account for a work-from-home scenario.

ADAPT THE CONTRACTING APPROACH FOR HIGH RISK SUPPLIERS

The FBI recently issued an alert[2] regarding the state-sponsored hackers "Kwampirs" (an international hacking group also known as Orangeworm) using malware to attack supply chain companies and other industry sectors as part of a global hacking campaign. The hacking group may have gained access to global hospitals through vendor software supply chain and hardware products. Infected software supply chain vendors included products used to manage industrial control system ("ICS") assets in hospitals. Similarly, the World Health Organization was targeted[3] by a state sponsored hacker in mid-March.

Ostensibly, these hackers hit the health organizations, hospitals, and suppliers while they were down as a result of the onslaught of activity caused by the pandemic. Limiting the amount of information that flows through these types of suppliers during the crisis may be prudent. In addition, for the data that will make its way to the high-risk suppliers, ensure suppliers are using the most recent PCI,[4] CIS,[5] SOC,[6] or other security controls and standards that take into account the COVID-19 environment.

ASSESSING AND UPDATING SUPPLIER PERFORMANCE AND COMPLIANCE

As part of a reentry to the new "normal" following these initial stay-at-home orders, customers should consider how to conduct assessments on what worked, what did not, and how to address risks posted by the remote-working protocols during the COVID-19 outbreak. Overall compliance checks with existing and revised corporate policies should be considered, as well. That said, these efforts for additional assessments and checks should not overlook the realities of the current circumstances – for example, by streamlined audit requests across an organization to avoid inundating suppliers with requests, along with an understanding that remote and virtual access is likely the only option for receiving information. Undertaking these efforts, even if only with the most significant suppliers, can not only help better prepare should similar circumstances occur, but ultimately the lessons learned will help to better inform the relationship and address risk areas which may not have otherwise been evident or which became exposed during this COVID-19 outbreak.

OPERATIONAL RESPONSES TO SECURITY INCIDENTS

If a cyber incident unfortunately does occur on the cyber-system of an organization or its supplier, there are a number of operational mitigants, such as siloing access points to the breached system, and leveraging the known indicators of compromise to fortify the system, to avoid further damage. However, even if this unfortunate circumstance does not arise, putting in place training processes for personnel and clearly memorialized procedures now ensures swift and comprehensive responses in the future.

WORK FROM HOME SECURITY

While an organization's broader IT infrastructure, and that of its suppliers, is a major element in its data security, the individual users themselves

could also play a major role in fortifying against the current cyber threats. The sudden and precipitous shift to working from home has transformed the routine of most organizations' workforce. For example, in a recent interview, the chief executive officer of Verizon noted that Verizon's customers are now making double the amount of calls as compared to the highest peak during a typical year and the duration of those calls has increased by 33 percent. Customers are sending messages every day at the same rate as New Year's Eve. Because users' phones, computers, and home internet networks were not previously equipped for this kind of full-time secure remote working, there are a number of exploitable points of vulnerability. These are just a few:

> *Virtual Meeting Applications.* The use of virtual meetings during the pandemic have taken an astronomical jump. One online meeting platform reported monthly users of its video conferencing app surged from 10 million in December to 200 million in March. These applications are now used for college classes, yoga sessions, board meetings, and more, with many users sharing sensitive information during their calls. Unfortunately, the FBI reports these conferences are susceptible to breach, with some disrupted by pornographic and/or hate images and threatening language.

To safely operationalize virtual meeting applications, utilize a paid account with the full suite of security measures enabled. (Take into consideration the above supply chain and third-party network risks in order to best contract with providers of virtual meeting applications.) On an individual-user basis, never post meeting invites in public locations, and require passwords to enter the chat rooms. Use the controls that limit who can share their screen, lock questions or comments, and mute users if necessary. Finally, if video is not required, change the settings to automatically disable the camera, and cover the camera eye on the computer or phone.

Increased Phishing Scams. Recently, the FBI's Crime Complaint Center reviewed over a 1,000 unique complaints related to online COVID-19 scams. Frequently, online scams leverage links in emails to redirect users to a download that includes malware or a virus, known as phishing. As inboxes are inundated with COVID-19-related updates, cyberattackers capitalize by posing as businesses or public institutions providing virus-related information. To combat this threat, organizations should remind individuals of the dangers of phishing schemes. When clicking through emails, users should ensure email addresses are spelled correctly, and from known senders. They should handle links with care, only clicking on vetted links, and when in doubt, running the email by IT departments.

Home Networks. Home internet networks are not normally equipped to process the size or sensitivity of a business's information. With

increasingly connected household items, the number of connection points are high, and often the security for those nodes are low to non-existent. Here are just a few risk-points on a home network:

- *Software downloaded from untrustworthy sources.* Printer drivers, group chat applications, and the like often come with internet downloads available. However, these third-party websites may not always be approved by an information technology team, and therefore pose a risk if downloaded. On an enterprise-level, consider instituting administrative controls prohibiting download of applications onto devices used for work purposes without administrative approval.

- *Updates and Patches.* When trusted sources do push updates or patches, download them. These enhancements may provide up-to-date protection of the system against new vulnerabilities.

- *Secure the IoT.* Many devices connect to home networks, from refrigerators, to baby monitors, to document scanners. Consider moving devices processing sensitive information to a separate network than, for example, a Roomba that currently picks up the remnants of your quarantine snacks. The same goes for minimizing the use of personal email for business, as the personal system may not have sufficiently robust security controls.

- *Minimize Family Sharing.* Allowing roommates, children, or partners to access your work devices creates its own security risk. While you can likely trust your loved ones not to steal company secrets, children are often not informed on cybersecurity risks, and sharing devices with an unknowing third party obfuscates your own safety and conscientiousness.

CONCLUSION

The first priority during this global crisis is to stay physically safe and healthy. As we endeavor to flatten the curve, we are learning to live and work in a very different environment. Unfortunately, the landscape for cyber related risks and pitfalls quickly changes. The dangers to networks and their users are seemingly endless and vary by organization and industry. This new normal means there are a new set of cybersecurity risks to care for. But a proactive and educated approach to a safe virtual lifestyle, with awareness of effective work from home security, and security of service providers, is vital.

NOTES

1. "Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments," FBI Public Service Announcement, *available at https://www.ic3.gov/media/2020/200401.aspx*.

2. "Kwampirs Malware Employed in Ongoing Cyber Supply Chain Campaign Targeting Global Industries, including Healthcare Sector," FBI Private Industry Notification, *available at https://assets.documentcloud.org/documents/6821580/Kwampirs-PIN-20200330-001.pdf*.

3. "Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike," *available at https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN*.

4. *https://www.pcisecuritystandards.org/covid19*.

5. *https://www.cisecurity.org/white-papers/resource-guide-for-cybersecurity-during-the-covid-19-pandemic/*.

6. *https://www.aicpa.org/eaq/covid19.html*.