Oh, and One More Thing, Cybersecurity: A COVID-19 Checklist

March 26, 2020 Tim Newman

PRACTICES Litigation, Internet, Privacy and Cybersecurity

As if businesses did not have enough to worry about during this COVID-19 pandemic, it's times like these when cybersecurity risk is at its peak. Distracted employees may be psychologically vulnerable to attack, and shifting quickly and unexpectedly to a remote workforce can create technology and control risks. It's a perfect storm for cyber risk.

If you can manage one more thing on your "to do" list, here are some things your organization can do to help minimize the risk of a cyber incident.

- **Make sure your employees are on high alert for scams.** Your employees are still your first line of defense against a cyber attack. Right now, they're stretched and distracted, and bad actors are exploiting COVID-19 fears to launch an increasing number of attacks. Train and re-train your employees to be on the lookout for phishing scams and other types of social engineering, and test them on their ability to suss out attacks. Remind them to not click on email links or attachments without scrutiny and to pick up the phone to confirm the details of wire transfers, especially if they receive instructions to change wiring information. Finally, reinforce the need for prompt reporting of any suspicious activity, and make sure employees know how to do so in a remote environment.
- **Give employees the tools they need.** Make sure your employees have the tools they need to access company information securely. That includes not only devices and security software, but also training and instructions on how to work remotely and maintain security in alignment with company policies. If employees don't have company-issued devices, make sure their personal devices and home Wi-Fi networks have adequate security and that employees know how to use them securely. If employees cannot access the information they need securely, they may find a workaround that's not secure.
- **Ensure remote work set-ups are secure and reliable.** Make sure employees accessing company systems do so securely, for example through virtual private network (VPN) connections. Make sure those VPNs are updated and patched, and make sure they can handle the increased traffic. Again, employees who can't get secure access to information often find other means. If you have not instituted multi-factor authentication, consider doing that now.
- **Monitor your network traffic.** Monitoring for intruders may be more difficult with more users accessing your network remotely, but keep an eye out for suspicious activity in your access and event logs, and continue monitoring for malware and other attacks. Emails to personal email accounts or downloads of large amounts of data may require closer inspection.
- **Support your IT staff.** Your IT staff will be stretched to support remote working, all the while carrying on its normal duties, including cybersecurity. Consider adding additional staff and rotating duties to keep your IT team fresh and at the top of its game.
- **Review incident response plans.** Incident response plans do not always account for a remote response. Make sure employees know how to report issues, and make sure your plan accounts for remote means of communicating with your internal team and outside providers. Company email may not always be available, reliable, and secure. If you have not

preselected legal, forensic, and other providers, do so now, and make sure you can reach them remotely.
- **Revisit your policies.** Revisit policies at a time like this? Yes. Review existing policies to make sure they account for remote working and any relevant COVID-19 guidance from regulators. If they don't, consider drafting some basic guidelines for employees to follow to ensure proper data security. After the storm clouds clear, promote these guidelines to a formal policy with any lessons learned from this experience.

These are just a few of the considerations that should be on your mind with respect to cybersecurity. Although some regulators have announced some flexibility in enforcement and penalties (see, e.g., our coverage of HHS's HIPAA Guidance During COVID-19), companies should operate as if all privacy laws still apply in full effect. Even if regulators ultimately give a breach victim a regulatory pass in light of COVID-19, the cost of investigating and mitigating a cyber incident can still be tremendous.

If you have questions about the impact of COVID-19 on your organization's cybersecurity practices, or if you have suffered a cyber incident, contact a member of our Privacy and Data Security Team below. You can also check out our COVID-19 Resources page and our Privacy and Data Security Practice Group Page for more information.