BRETTNER
CVITANOVIC

CYBER 101 FOR LAWYERS: COVID-19 EDITION

BY: DOMINIK CVITANOVIC AND JACQUELINE BRETTNER

BRETTNER CVITANOVIC, LLC

The legal work environment has been slowly shifting to distributed workplaces for several years. First, smartphones enabled lawyers to work on the go, and then the advent of tablets and docking stations made law offices truly mobile. This mobility also came with strings, as lawyers ethically must take reasonable action to maintain the privacy of their clients' information. Therefore, law firms had to analyze cyber threats and how a growing number of remote workers would impact their data flows. COVID-19 has taken this "growing number" and turned it upside down. Now, unless deemed "essential", lawyers are *all* working remotely from home, and the same data privacy/cybersecurity concerns affecting businesses across the country are also affecting law firms.

First, law firm servers are getting the ultimate stress test to see if they can withstand the higher volume of traffic. If you know that your employees are complaining about the speed of their connection to your billing system, document management system, or other internal servers, take these complaints seriously. Slowdowns in workflow can result in employees getting frustrated with cybersecurity protections that may be slowing their connections. More than most, lawyers and their employees are under pressure to meet deadlines, and employees might use personal email or unencrypted connections to get things moving faster. Employees should be warned against this action, while employers should take care to improve their digital bandwidth.

Second, employees are likely using their personal devices more than ever to conduct business work. This opens that work to potential threats, especially if they have not been provided with and/or warned to use Virtual Private Networks ("VPNs"). VPNs allow users to share data on public networks as if the devices were directly connected to a private network. Now that employees are not connecting to law firm's internal networks but instead home networks that share connections with devices all over their homes, employees should be given instructions on basic wi-fi security tips.

For example, wi-fi networks should not use simple or default network passwords, should not keep the default network name (as this identifies the type of router you have), and should use WPA2 encryption if WPA3 is not available. Lastly, your router can likely be accessed online through an admin password. You should also change *this* password from the default setting to avoid third parties from accessing the back-end router set-up and changing your network password. These are just a few of the easy (and free) steps that can be taken to further solidify home network security. Since lawyers are now using these networks for personal and business use, lawyers must be aware of these simple ways to

harden their defenses against cyber incidents from the significantly higher usage of home networks for firm work.

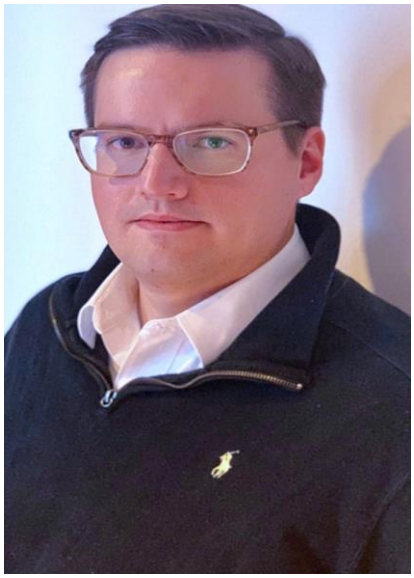
Third, some businesses built their data integrity infrastructure on the assumption that most business would flow through the local private network at their place of business. Now, depositions and client interaction are taking place over Teams, Zoom, Skype, Google Hangout/Meet, or other video conferencing applications. Law firms are now trusting third-party programs more than ever to handle sensitive information. For years prior to COVID-19, cyber professionals have advocated for multi-factor authentication on top of unique passwords to strengthen the security of employers' online platforms. That has not changed. The multi-factor authentication requirements in place for law firm email and document management systems must be extended to new programs taken on during this crisis, including video conferencing programs.

Even with strong passwords and multi-factor authentication, law firms must choose their video conferencing programs wisely. Zoom saw a boom over the last several weeks due to a need for a user-friendly way for people to talk to family, co-workers, and clients remotely. However, the notoriety also led to heightened scrutiny of Zoom's platform, leading New York City public schools to ban Zoom meetings due to safety and security concerns, instead opting for Google's platforms or Microsoft Teams. New York City's reaction is merited, as zero-day exploits were revealed last week, one of which allowed attackers to tap into a user's webcam and microphone without permission. Further, if users distribute meeting numbers, "Zoom bombers" can crash into meetings and share shocking images or otherwise disrupt meetings. There are ways to avoid this already in Zoom such as restricting access through use of a waiting room, requiring a password to access the meeting, locking the meeting after it starts, and also restricting file transfers or screen sharing to meeting hosts.

More importantly, if you have a smaller webmail provider (not Gmail, Outlook, etc.), then Zoom's system may be automatically placing everyone using that email domain into a company folder where everyone in that folder has shared access to email addresses, user names, and user photos. Also, it has been reported that Zoom's meeting transcripts (including private chats) are available to the host at the end of the meeting, so if you wish to have a private chat with your client during a Zoom mediation, it is likely best to have a separate meeting entirely for privileged communications. Late last week, Zoom's CEO pledged to fix its flaws (and there are many), so before using Zoom for client information, consult a security professional to determine that it is safe for use. At this time, we cannot verify that all of Zoom's reported flaws have been repaired.

Lastly, just like businesses, law firms should take this time to refresh employees on their firm's employment information security policies, cybersecurity best practices, bring-your-own-device policies governing employees' personal devices, and/or cyber incident response plans. If you don't have any of those, it may be time to consult with a cybersecurity attorney in your area.

Jacqueline M. Brettner is a data privacy advocate. She is the founder of the firm's Cybersecurity & Data Privacy Practice and has over ten years of experience handling data and privacy related risk management and associated insurance coverage litigation. Jackie can be reached at brettner@bcfirm.law or by phone at 504-782-1166.



Dominik J. Cvitanovic has experience in cybersecurity audits of client data flows and best practices and procedures to ensure compliance with state, federal, and international law, including the European Union's General Data Privacy Regulation and the California Online Privacy Protection Act. Dominik can be reached at cvitanovic@bcfirm.law or by phone at 504-952-5866.