Ten Cybersecurity Lessons Learned About Working from Home

By Sharon D. Nelson, Esq. and John W. Simek

The year 2020 will be remembered as the year lawyers were catapulted into the future. As a result of COVID-19, most law firms were suddenly thrust into a work-from-home environment. Some were prepared for working remotely, but many were not. We've helped a lot of lawyers transition to different working environments by providing training and implementing new technologies in their practices. Along the way, we've learned some things about how lawyers have responded to the pandemic. Here are 10 cybersecurity lessons we've learned about working from home.

1. Home networks are 3.5 times more likely to have at least one family of malware than corporate networks.

A study by BitSight, a cybersecurity ratings firm, analyzed data from 41,000 U.S. companies. They found that 25 percent of devices (e.g., printers, computers, Internet of Things devices, etc.) on a home network had services exposed to the internet. Another scary statistic from the study: 45 percent of the organizations had one or more devices accessing its corporate network from a home network with at least one malware infection.[1]

Ouch.

2. Sharing devices you use for work with family members is a bad idea.

Devices used to access your law firm network and work on confidential client data should only be used for that purpose. Family members should not use the same device even if users have separate login IDs and passwords. If a family member inadvertently performs an action that leads to installation of malware, client data and law-firm access could be compromised.

3. Zoom is currently the choice of clients and potential clients.

Teams, Webex, Zoom, and GoToMeeting are all good video conferencing platforms. In our experiences, Zoom is the technology of choice for current and potential clients. The other platforms are playing catch-up to Zoom. Despite some early histrionic media reports, Zoom can be used securely for client communications.[2]

4. Make sure your confidential client conversations are kept private.

Many of us are sharing working space in our homes with others. As a lawyer, you have an obligation to ensure that client conversations are private. That means having a separate room to conduct client conversations; consider using a headset, too. You wouldn't loudly discuss a client matter while commuting on the train, so why would you allow family members to eavesdrop?

5. Employee security awareness training is more important than ever.

Working from home has put law firm employees into situations that carry different risks from when they were in the firm's office, so we need to be even more diligent with safe computing practices. Cybercriminals know there are a lot of targets working from home using insecure home networks. Training employees to recognize current cyberthreats is an absolute must.

Working from home has put law firm employees into situations that carry different risks from when they were in the firm's office….we need to be even more diligent with safe computing practices.

Law Practice Solutions is a regular feature brought to you by the Practice Management Resource Center (PMRC) of the State Bar of Michigan, featuring articles on practice, technology, and risk management for lawyers and their staff. For more resources offered by the PMRC, visit our website at http://www.michbar.org/pmrc/content or call our Helpline at (800) 341-9715 to speak with a practice management advisor.

6. Have a work-from-home policy.

If you don't already have one, now would be a good time to develop a work-from-home policy that sets employee expectations and spells out what they should and shouldn't do. Specific technology requirements may be part of the policy, too. The policy can also include a statement about family use of devices to further support the second item on our list.

7. Consider issuing firm-owned laptops so you control the security of devices used at home.

More and more of our clients are not purchasing desktop computers but opting for laptops or tablets with docking stations as the primary computing device. That approach makes migrating to a work-from-home environment much easier. A firm-owned laptop is configured with the security software and applications the user needs to perform their job. Using the laptop on the home network preserves the security of the computer, making it safer than the typical home machine.

8. There are options for home users competing for bandwidth.

If you're working from home, your spouse is probably working from home, and your children may be attending school remotely as well. This means you are probably sharing the same wireless network as everyone else and experiencing slowdowns. You may try using the hotspot on your mobile phone to see if speeds are better than your home network. Connecting your computer directly to your router via Ethernet will help maximize speed. If you don't have Ethernet cabling in your walls, try an Ethernet powerline adapter. At around $50 on Amazon, the TP-Link AV1000 is a good choice, although we have found that pricing and availability are all over the place.

9. Use a virtual private network (VPN) for remotely connecting to the firm network.

Using a VPN is better than not using one. A VPN creates an encrypted communication channel from your computer to the firm network. Many users will be tempted to use remote desktop protocol (RDP) since it is included free with Windows, but there are many known vulnerabilities with various versions of RDP. If you must use RDP, consider running RDP through a VPN tunnel instead of exposing RDP directly to the internet and, by all means, use multi-factor authentication for any connection.

10. Prioritize lawyer wellness.

Lawyers struggling with wellness are a security risk. Lack of concentration, mental health problems, or substance abuse can cause serious lapses in making smart decisions concerning the use of technology. ■

Sharon D. Nelson, Esq. is a practicing attorney and president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association, and the Fairfax Law Foundation. She is a co-author of 18 books published by the American Bar Association. She can be reached at snelson@senseient.com.

John W. Simek is vice president of Sensei Enterprises, Inc. He is a certified information systems security professional and a nationally known expert in the area of digital forensics. He can be reached at jsimek@senseient.com.

ENDNOTES

1. *Rush to Work from Home Exposes Alarming Security Issues, BitSight Research Shows*, BitSight (April 14, 2020) <https://www.bitsight.com/press-releases/rush-to-work-from-home-exposes-alarming-security-issues> [https://perma.cc/TY5N-MB9N]. All websites cited in this article were accessed October 10, 2020.
2. E.g., Wagenseil, *Zoom security issues: Here's everything that's gone wrong (so far)*, tom's guide (September 2020) <https://www.tomsguide.com/news/zoom-security-privacy-woes> [https://perma.cc/3KEY-QGJB] and Warren, *Zoom faces a privacy and security backlash as it surges in popularity* (April 1, 2020) https://www.theverge.com/2020/4/1/21202584/zoom-security-privacy-issues-video-conferencing-software-coronavirus-demand-response.