Affinity Programs

PROFESSIONAL COUNSEL℠

Advice and Insight into the Practice of Law®

The Remote-Ready Law Firm: Managing the Long-Distance Relationships

Introduction

Good lawyers have their best suit at the ready, but may just as often don slippers and sweatpants. Seventy-two percent of lawyers telecommute at least some of the time according to the American Bar Association's latest *Profile of the Legal Profession*.[1] As legal technology grows more accessible and digital natives become the dominant group in the American workforce, one should only expect this percentage to rise.

Coworking spaces, cloud computing and virtual receptionists have allowed some law firms to ditch their offices entirely. Most lawyers, however, seek a middle ground: a practice capable of functioning remotely when convenient or necessary, but still anchored to a physical office. The benefits of creating a remote-capable business are well worth the investment, enabling a firm to maximize productivity when traveling, attract top-level talent, and maintain functionality during a crisis.

Seventy-two percent of lawyers telecommute at least some of the time.

– American Bar Association
Profile of the Legal Profession

Minimizing Paper

If the firm does not currently have a system for doing so, digitizing client files may be the most burdensome aspect of a remote-work upgrade. Even with a system already in place, ensuring that lawyers can work remotely may require more extensive or consistent document imaging practices. All physical documents that comprise a file should be scanned, saved and, unless the original *must* be preserved, shredded. Lawyers should prioritize active files, with an emphasis on streamlining current and prospective workflows before tackling the mountain of closed files in storage. Remember: the goal is to facilitate remote work, not to devise a one-hundred percent paperless office, which is seldom realistic.

Depending on the volume of documents and the composition of the practice, digitizing paper files may be accomplished by in-house staff. Firms may instead consider using a third-party imaging service, especially if they intend on digitizing decades of old boxes. In any event, whether independently or in consultation with an outside vendor, lawyers must ensure that electronic files are properly labeled, organized, legible, and retrievable, which requires careful planning and the right equipment. For more on this issue, see the CNA resource *Creating a File Retention and Destruction Policy*.

1 American Bar Association. *ABA Profile of the Legal Profession*, 10 Aug. 2019.

Server Decisions

Digitizing files will reduce the cost and aggravation associated with keeping a forest's worth of paper in a back room or offsite storage facility, but even electronic files must be stored somewhere. The default option for law firms has long been on-premise servers, which require major upfront hardware and installation costs, but allow for complete control over the security and privacy of firm data. The value of that control, however, depends greatly upon the firm's IT expertise, which generally requires an outside consultant, as well as the firm's commitment to its own security protocols. As the practice grows or as hardware becomes outdated, on-premise servers will likely require additional investment from the firm.

The alternative to on-premise storage, of course, is cloud storage. Most lawyers, 58 percent according to the ABA's most recent Legal Technology Survey Report,[2] now employ cloud-based services in their practice. Undeterred and probably partially motivated by the lack of direct control over data privacy and security, lawyers opting for a cloud-based solution outsource those responsibilities to a third-party vendor. The cloud provider guarantees the integrity and accessibility of firm data, protects it from outside intrusion, and shoulders hardware costs for a monthly or annual fee. Vendors dedicated to the legal industry often provide document storage and practice management software as an all-in-one, fully integrated service.

Between firm-owned, privately managed on-premise servers and rented space within public, multi-tenant cloud servers lies a third option: a private cloud. Like more familiar public cloud-storage solutions, private clouds outsource the responsibility of owning and maintaining a server to a third-party vendor. In contrast to a public cloud, however, firm data in a private cloud is stored on a dedicated, single-tenant server, separate from other customers' data. In addition to greater control over how firm data is managed, this allows the firm to host its software, documents and email on one platform, but at the same time places the burden of security largely on the firm itself.

Secure Access

The manner in which firm employees can securely access firm systems and data depends on how the firm has chosen to host those systems and data. Firms using their own dedicated servers, whether they are on-premise servers owned by the firm or servers maintained by a third-party vendor as a private cloud, generally use a virtual private network (VPN) to facilitate individual remote access. Other methods for remote access, including Remote Desktop Services or a Virtual Desktop Infrastructure, tend to be a worse fit for law firms given their higher cost, added upkeep, inferior security, and less flexible user experience relative to a VPN.

A VPN connects one private network to another private network, commonly using encryption to ensure the connection is secure. Although several variations exist, a lawyer working remotely can connect to the firm's network by using a client-based remote access VPN. In simplest terms, this creates a secure tunnel between the lawyer's local network on one end and the firm's network on the other end across a public network (the internet). Data traveling within the tunnel is encrypted and, if intercepted, is indecipherable. Lawyers log on to the VPN client and are granted access to data and systems on the firm network as if sitting at their desk.

Where firm storage and services are cloud- or web-based a VPN is not necessary. A lawyer working from home who logs on to Microsoft Exchange Online, Clio, or other services with infrastructure independent of the firm has initiated a secure connection to that provider's servers. In effect, access to these servers is always "remote," even when the lawyer is at the office. As with any password-based application, however, strong passwords and multi-factor authentication are vital.

Public Wi-Fi

Countless warnings have been issued about the free Wi-Fi networks offered by hotels, airports, coffee shops and other public places. The primary threat is an attacker positioned between a user and the connection point, allowing this so-called "man-in-the-middle" to intercept the user's data on its way to the destination server. This data might include sensitive emails, financial information, or the security credentials to the firm's network.

Over the last decade, however, websites have steadily implemented HTTPS ("Hypertext Transfer Protocol Secure"), an encrypted internet protocol that protects the communications between a user and a site. As of May 2020, HTTPS accounts for 95 percent of connections from Google Chrome users in the United States,[3] up from

2 Kennedy, Dennis. "2019 Cloud Computing." *ABA TechReport*, 2 Oct. 2019.

3 Google. "HTTPS encryption on the web." *Transparency Report*, 2 May 2020.

a mere 50 percent as recently as 2014, encompassing virtually all commercial and social networking websites. Web browsers have also made significant strides in terms of signaling and defending against potential attacks. In light of this progress, the Electronic Frontier Foundation, a leading digital privacy nonprofit, has opined that "advice to avoid public Wi-Fi is mostly out of date and applicable to a lot fewer people than it once was."[4] This assumes, however, that a user is running adequate firewall and anti-virus software and has kept web browsers and operating systems up-to-date.

From a security standpoint, public Wi-Fi has substantially improved, but it is far from perfect. HTTPS is still not universally deployed by default; communication with sites using only HTTP, the unencrypted predecessor of HTTPS, remains vulnerable to interception. Every major web browser will warn the user, generally within the address bar, that a connection to a website is not secure. For greater security, lawyers might consider using "HTTPS Everywhere"[5] or a similar browser plugin that rewrites requests to websites using HTTP as HTTPS where possible.

By no means has the widespread transition to HTTPS rendered public Wi-Fi attacks impossible. It has, however, made them much easier to defend and more difficult, and thus less worthwhile, for an attacker to execute. Ransomware and phishing attacks have become far more lucrative than trolling for telecommuters in a hotel lobby.

Regardless, the more comprehensive approach to public Wi-Fi security involves a VPN. Lawyers who use a remote access VPN to connect to their firm network can use that same VPN to protect their traffic and conduct firm business on public Wi-Fi. Those without the need for an existing remote access VPN may instead use a commercial VPN. Instead of securely tunneling data from the lawyer to the firm's network, a commercial VPN securely tunnels a user's data to its own network before relaying it on to the intended destination, and vice versa. In this way, the commercial VPN shields a user's traffic from anyone else on the same public Wi-Fi network.

All VPNs are not created equal, however. Commercial VPNs may themselves have security flaws and lawyers must consider whether the VPN provider, and the country in which it is located, can be trusted to respect the privacy of their data. Free options, generally, should not be considered for business use.

VoIP and Video Calls

The era of landline phones has all but ended. As consumers have replaced their analog phones with digital cell phones, businesses have steadily migrated to VoIP ("Voice over Internet Protocol") systems, which convert analog voice signals into digital signals and transmit them over the internet.

Traditionally, a lawyer could receive calls remotely by having office calls forwarded to a cell phone or by maintaining separate work-designated cell and office numbers. A VoIP system, however, allows a lawyer to direct all work calls to a single, unified number across several devices. Moreover, with few exceptions, the firm's existing number can be ported to the VoIP service. VoIP calls can be made using software on a PC, generally with a headset for improved clarity, but also any smartphone or even an analog phone equipped with an adapter. Lawyers have their "office line" with them wherever they happen to be working, most often at a considerably lower cost to the firm.

Video calls have likewise made significant headway with both consumers and businesses as a way to conduct virtual meetings, never more so than during the spring of 2020 in the midst of the coronavirus pandemic. The videoconferencing service Zoom, in particular, appealed to users with its intuitive interface, crystal clear video and sound quality, and attractive pricing, including a free tier for calls up to forty minutes.

Users quickly realized, however, that Zoom was rife with security flaws: despite assurances to the contrary, calls were not encrypted end-to-end, the transport encryption the company did offer was less secure than advertised, and encryption keys could be issued by servers in China even where all participants were in North America.[6] Zoom was also caught sharing user data with Facebook, even relating to users without a Facebook profile, resulting in a pending class action lawsuit.[7]

Zoom's missteps underscore the importance of vetting the firm's vendors. How is the vendor protecting calls from intrusion? Where are the servers located? What data is stored, who will have access to that data, and how can it be used? Zoom has vowed to improve its privacy and security practices, but users making particularly sensitive calls, lawyers among them, should look elsewhere unless significant strides are made. Apple's FaceTime, Google's Duo and Cisco's Webex all support end-to-end encryption, meaning the provider itself cannot access call data even if it wants to. And while these companies offer free versions, lawyers are wise to remember the maxim, "if the product is free, then you may be the product."

4 Hoffman-Andrews, Jacob. "Why Public Wi-Fi is a Lot Safer Than You Think." *Electronic Frontier Foundation*, 29 Jan. 2020.
5 *See* https://www.eff.org/https-everywhere
6 Lee, Micah. "Zoom's Encryption is 'Not Suited for Secrets' and has Surprising Links to China, Researchers Discover." *The Intercept*, 3 Apr. 2020.
7 Bond, Shannon. "A Must For Millions, Zoom Has A Dark Side—And An FBI Warning." *NPR*, 3 Apr. 2020.

Device Management

The best way a firm can ensure remote workers are equipped with effective, properly secured hardware is for the firm to issue the hardware itself. If the firm owns the device, it can exercise complete control over acceptable use and software or application downloads at all times, regardless of whether the employee is connected to the firm network. Implementing anti-virus, firewall, device encryption, data backups and other security measures is easier when devices are uniform throughout the firm, as are device and software updates.

The obvious downside of providing employees with hardware is the cost. Permitting employees to use their personal devices for firm business, in whole or in part, spares the expense and hassle of purchasing and upgrading those devices and lets employees use devices they already know and like. However, even with a carefully drafted bring-your-own-device (BYOD) policy, the line between firm time and personal time can blur, and both the firm and the employee must understand their rights and responsibilities as far as data privacy, security, and maintenance. What security measures will the firm require? Will employees be reimbursed for usage and data costs? What level of device support will the firm provide?

Whether devices are owned by the firm or the employee, the firm needs a policy to address a lost or stolen device, as well as the related issue of an employee's departure or termination. In both circumstances, the ability and authority to wipe firm data from the device, remotely if necessary, is critical. Employees are understandably more prone to carry in public, and lose track of, a personal device. Mobile Device Management software can make this process quick and painless, but the firm's rights with respect to data removal and the corresponding risk to personal data on the device should be addressed up front in writing.

Conclusion

For law firms of any size, taking steps toward remote-work capability often means greater firm productivity, reduced costs over the long term, and a leg up in hiring and employee retention. In times of crisis, it may very well be the difference that keeps your business afloat.

For information on vendors that may help your firm work remotely, please consult CNA's Lawyers' Allied Vendor Program.

This article was authored for the benefit of CNA by:

Matthew Fitterer

Matthew Fitterer is a risk control specialist for CNA's Lawyers Professional Liability program. He provides risk control guidance to CNA insureds in the form of written publications, training seminars and direct consultations. Prior to joining CNA, Matt practiced law at a Chicago-area criminal appeals and civil rights firm, and later at a firm specializing in commercial litigation. He received his bachelor's degree from the University of Illinois at Urbana-Champaign and his law degree from Chicago-Kent College of Law. He is licensed to practice in Illinois. Matt has been designated as a Commercial Lines Coverage Specialist (CLCS) by the National Underwriter Company and a Certified Information Privacy Professional (CIPP/US) by the International Association of Privacy Professionals.

For more information, please call us at 866-262-0540 or email us at lawyersrisk@cna.com