FOCUS: CYBER SECURITY

Cyber Security in 2023 is an All Hands On Deck—Everybody Thing—Not Just an 'Office IT' Thing!

Nicholas Himonidis

It's 2023. Do ***you*** (not your office IT person) know where all your sensitive data is? Do ***you*** know (remember, and keep track of) all the various ways of accessing it? If not, you probably are not doing enough to ensure your data stays secure.

As attorneys, we generate, send, and receive a great deal of sensitive and legally privileged data. We (not our 'office IT people') are legally and ethically responsible for the security of that data. On a more practical level, the 'dataspheres' we operate in today are such that without the direct and meaningful participation of every end user (every attorney/assistant/paralegal in the firm), the most herculean efforts of the most competent IT people will not be sufficient.

Many attorneys do not know where all of their sensitive data lives—and perhaps more importantly—do not keep careful track of the myriad ways they access that data. Most attorneys are too busy with day-to-day case work to give these questions serious thought—and that is a dangerous mistake.

Most would probably say their data is stored on a "secure" email server or a "secure" file server or it's "in a secure cloud environment"—or that they have an IT company that "secures" their data. But the formidable cyber security defenses of the big data platforms we use, and the 'network security' that our IT professionals are primarily focused on, are NOT how most data breaches occur today. Vulnerabilities in end user devices (frequently personal devices), and compromises of account login credentials are among the most common attack vectors exploited by hackers.

Attorneys are prime targets for hackers. According to a 2021 ABA survey, 25% of respondents reported that their firms had experienced a data breach at some time.[1] That number increased to 27% in 2022.[2] One recent action by the New York State Attorney General's Office against a New York medical malpractice firm that fell victim to ransomware resulted in a $200,000 penalty and a requirement to implement data security improvements.[3]

Understand Your Data Ecosystem

Securing your data starts with knowing where your data is, and all of the ways to access it. While this concept may seem overly simplistic, many business owners, including attorneys, do not know where their sensitive data resides, much less consider the platforms and services through which it passes daily. We all have smartphones and computers, likely with multiple email accounts on each.

Our phones have apps for both work and personal use. We subscribe to services like Zoom, Dropbox, OneDrive, etc. Our smartphones and tablets, not just our office computers, are linked to email servers, file shares, cloud storage systems, databases, and other applications. Nearly every device we use has sensitive data stored on it, passing through it, or is a conduit to access that sensitive data.

Knowing where the sensitive data is stored, and what devices and apps can access that data, is the first, and most critical step to securing that data. Why? Because hackers frequently target the weakest attack vector (or point of entry)—and most often that's YOU—the end user. Why should they break through a solid steel door if they can easily steal the key from someone who is careless with it, and perhaps forgot they even had it? You, the 'end user' must develop good cyber security habits on your smart phone, your home computer, your iPad, etc.—or you will continue to be the 'weak link' in the cyber security battle.

Let's discuss some specific actions you can and should take to help protect your sensitive data.

Smartphones

We communicate constantly on our phones, by voice, text, and email. Many of us also use messaging apps—Facebook Messenger, Instagram, WhatsApp, WeChat, Snapchat, Telegram, Signal, Viber, etc.—in addition to enterprise messaging platforms, like Slack, Teams, or Discord. Then, we have email platforms and services, such as Exchange, Gmail, Yahoo, AOL, ProtonMail, Tutanota, and others. Of the many apps on our phones, most of us use only a few regularly; the rest are completely forgotten, and that is a vulnerability in and of itself because unused apps are not regularly updated—and 'security fixes' don't get applied.

So where do we start? First, secure the phone itself. Make sure you have a secure passcode coupled with screen auto-lock set to a very short period (like one minute). Next, consider taking the following steps:

- Review all apps and delete those that are no longer used.
- Configure the operating system and all apps to update automatically.
- Review the privacy settings for all apps, especially those with which you share your location, contacts, photos, camera, or microphone.
- For apps with access to sensitive data, enable an app-specific PIN code (different from your phone passcode) or use biometrics, such as a fingerprint or facial recognition, to access the app, if available.
- Enable the ability to remotely lock, locate or wipe the device if it is lost or stolen.
- Contact your cell carrier to place extra security on your account, such as requiring a passcode for authorized users to make changes, which will protect against increasingly common SIM swapping attacks to bypass SMS based 2FA (more on this later).

Company-issued cell phones are likely being managed by your IT group, using a mobile device management (MDM) platform that enforces policies in line with industry best practices—but the vast majority of attorneys 'BYOD'—bring their own device—and must therefore accept responsibility for the security posture of that device.

iPhone users need to understand how iCloud works and take steps to avoid inadvertent "spillover" of iCloud data to any device not used and accessible exclusively by you. The data in your iCloud can sync to any Apple devices with the same Apple ID. Never enter your Apple ID and password into any Apple device that is not used exclusively by you—as your sensitive information may be synced to those devices. You should routinely review the list of devices connected to your Apple ID—and immediately 'log out' any device you are not 100% is yours and can be accounted for.

Apple has released a new feature called "Lockdown Mode" in iOS (16)—which, when enabled, provides extremely high protection against digital threats. Attorneys who deal with particularly sensitive data, or routinely access client data from their iPhone may wish to consider engaging this extreme threat protection.

Computers

If you have a firm-issued laptop, it is likely managed through enterprise software that enforces security policies. However, if your laptop (or home desktop used for work) is not being managed this way, be sure to follow the guidelines outlined above for smartphones, and take these additional steps:

- **Enable full-disk encryption—*especially on laptops*.** This prevents anyone, including sophisticated thieves, from copying data directly from the computer's hard drive if it is lost or stolen. This is NOT the same as having a 'login password'—which is easily defeated by professionals. Windows and Mac both have built-in, whole-disk encryption, BitLocker on Windows and FileVault on Mac, but they need to be turned on in settings.

- **Activate a premium antivirus subscription** to provide real-time protection against threats from email attachments or web surfing. Many of us with personal computers either received a trial subscription to an antivirus program or downloaded a free version at some point; free and expired trial versions don't carry the same benefits as a premium program, such as real-time scanning, browser scanning, automatic scans, or automatic updates.

While your cell phone temporarily retrieves files stored elsewhere, computers operate differently, and actual copies of files viewed from a remote source often end up cached on the hard drive—another compelling reason to enable full disk encryption, should the computer be lost or stolen.

You need to understand what information is stored on your computer and where else it might exist. Most people are familiar with Desktop, Documents, and Downloads folders, but what about email? Let's say you use Microsoft Outlook. All the emails you read and search through have a local copy saved on that computer (and any other computers where you have Microsoft Outlook installed), including attachments.

That information also lives on the Microsoft Exchange server and the file server where Exchange is backed up. Even if you only access email from Microsoft Outlook using a web browser (formerly Outlook Web Access, or OWA), any attachments you open are stored on your computer as a cached file. Beyond email, other documents and files are saved in various locations on your computer. If you use Microsoft 365, for example, all that information syncs to Microsoft's cloud and is accessible wherever you log into Microsoft 365.

Much of the sensitive information you generate and receive—through email, shared drives, or local apps—exists in many locations, and you must consider how to protect every one of these potential "attack surfaces." Do not ever save login credentials for anything of importance in outlook contacts or notes.

Apps

Apps (on your phone or computer) make accessing all kinds of information easy and convenient, but that convenience comes at the cost of reduced security. Every app has potential vulnerabilities, and lesser-known apps often have far less built-in security, with updates that may be infrequent or non-existent. All apps must be properly configured for security and privacy, and all non-essential or rarely used apps should be deleted. Additional considerations are laid out below.

Accounts for Apps

When signing up for a new app, use your work email for a business-related app and a personal email for a personal app. Be extremely cautious about apps and accounts that offer the option to sign in with another account, such as Google or Facebook. Using this option relies on those other services to secure your login information. If one of those platforms does suffer a breach, and your credentials are compromised, whatever other accounts you signed into this way may also be compromised. Instead, create separate, distinct login credentials for each and every account you utilize (see below regarding the use of a 'password keeper').

Passwords for Apps

To generate and keep track of unique, complex passwords for all of your many accounts, consider a password manager such as RoboForm, LastPass, Dashlane, 1Password and others. These utilities offer the ability to automatically generate different, complex passwords for all of your accounts and store them in an encrypted vault. Even though password manager companies are a prime target for hackers, they are still very secure, and using them to store unique, complex passwords for all of your separate accounts is much safer than most of the alternatives. You just need to make sure that the 'master password' you use for your password manager is long, easily memorable to you but not 'guessable' by anyone else and is one that you have never used before. Commit that one master password to memory, and, if absolutely necessary, write it down and store it in one very secure place (like a safe).

Multi-Factor Authentication (MFA)

Also referred to as two-factor authentication (2FA) or two-step verification, MFA should never be ignored. Along with good password discipline—it is the single best defense against one of your accounts or 'gateways' to your sensitive data being compromised. Nearly all apps and services offer MFA, and if they don't, you should consider an alternative. Many apps and services offer multiple forms of MFA including SMS (text) codes sent to your cell phone, authenticator apps like Google Authenticator, biometrics, and physical hardware. SMS codes being texted to your phone is the weakest method of MFA—as this can be defeated by SIM swap attacks, which are becoming increasingly common, where a hacker tricks your carrier into porting your phone number to a phone in the hacker's possession—at which point they, not you, will receive the MFA code(s) via SMS. Wherever possible, use an authentication app, such as Google Authenticator, Microsoft Authenticator, or Duo. These are not 'SMS' based, and if you do become a victim of a 'SIM' swap—the hacker will not see the necessary MFA codes—but you still will have access to them.

Remote Access Apps

While the ability to access files or a computer remotely increases productivity and efficiency, it also increases risk. If using a remote-access application, such as TeamViewer, AnyDesk, Splashtop, or RDP, ensure that your credentials are not saved for automatic access, and enable authenticator app based MFA.

File Storage Apps

Apps and services such as OneDrive, Dropbox, ShareFile, Box, and others make it very convenient to access files anywhere, anytime, from any device. This same convenience also makes it easier for hackers to steal files. The devices used to access these apps must have proper security settings enabled, and the apps themselves need to be secured using proper password controls and MFA.

As lawyers, we are responsible for a great deal of sensitive data, and we must do everything we can within reason to help secure that data. With data breaches on the rise, and attorneys being prime targets, effective cybersecurity requires an 'All Hands on Deck/Everybody All In' approach.

1. https://www.americanbar.org/groups/law_practice/publications/techreport/2021/cybersecurity/.
2. https://www.americanbar.org/groups/law_practice/publications/techreport/2022/cybersecurity/.
3. https://ag.ny.gov/press-release/2023/attorney-general-james-secures-200000-law-firm-failing-protect-new-yorkers.

Attorney and cybersecurity/forensic expert **Nicholas Himonidis** is the CEO of The NGH Group, Inc., in Melville. He is also Co-Chair of the newly formed NCBA Cyber Law Committee.