How Attys Can Avoid Exposing Their Firms To Cyberattacks

By **Mark Hurley and Carmine Cicalese** (June 26, 2023)

Mark Hurley

Carmine Cicalese

The easiest way to breach a law firm is not to go directly after the firm. A much simpler path is to target individual attorneys, at home and on their personal devices. And a single misstep by only one attorney is all that hackers require.

More specifically, law firms are particularly inviting to cybercriminals. Attorneys regularly handle confidential and sensitive client information, something that can be sold or used to blackmail the firm for a great deal of money.

For example, information stolen in cyberattacks against Cravath Swaine & Moore LLP and Weil Gotshal & Manges LLP, reported in 2016, was used as part of a multimillion-dollar insider information trading scheme.[1] Cadwalader Wickersham & Taft LLP had its email system taken over by hackers last year,[2] and Genova Burns LLC was breached early this year, leading to the third time in the past six months that Uber has had client data stolen.[3]

According to a 2022 American Bar Association survey, nearly 27% of all industry participants have been breached.[4] Unsurprisingly, many law firms are now taking steps to upgrade their cybersecurity.

However, cybercriminals continuously evolve their tactics. They study their targets and prey on tendencies to find the weaknesses in security structures. They also recognize that, although law firms are more conscientious about cybersecurity, large numbers of attorneys still largely ignore it on a personal level. And it is this gap between work and personal that hackers exploit.

Indeed, attorneys regularly work remotely, including at night and on vacations. Another 2022 ABA survey found that 87% of law firms allow this in the post-pandemic era. Moreover, 30% of attorneys almost always work away from the office.[5]

Many firms have protected themselves by preventing personal devices from accessing anything beyond work email accounts, allowing only company-issued computers to access other confidential client information. Unfortunately, this structure is very expensive, cumbersome and often impractical for smaller law firms. Plus, it is far from bulletproof from cyberthreats.

For example, work email accounts often contain large amounts of confidential information, and there have been numerous recent instances of personal devices being stolen with their passcodes.

Cybercriminals target individuals who do not carefully shield their device passcodes when entering them in public places such as a bar or restaurant. Criminals can memorize four- to six-digit codes and simple swipe patterns as they are entered. At a later, more opportune moment, the criminal will steal the device and can access everything on it, including the attorney's work email, provided it can be accessed without an additional password.[6]

There are also instances when a client needs something completed immediately and the attorney does not have a work device handy. Consequently, some will make one-time exceptions from firm policies and find a way to download work information to a personal device or send it to a personal email account. But a one-time exception is all that a hacker needs to breach the law firm's cyber protections.

Consequently, hackers regularly target attorneys' personal email accounts. They typically have a fraction of the cybersecurity protections of their work counterparts. Once in, cybercriminals can search for information sent to the account from work. A single deal or litigation file is a potential gold mine.

Even if the personal email account has no work information, breaching it creates opportunities for spear phishing — i.e., sending emails ostensibly from a known or trusted sender to targeted individuals. Colleagues and clients will often open emails and accompanying attachments sent from an attorney's personal account. When they do, the recipient's systems can be infected with malware — i.e., software that gets behind cyberdefenses to steal information or that takes control of systems.

Trojans are a class of apps that may look legitimate but instead are designed to spread malware. They can be downloaded in seconds onto a briefly unattended device at a conference or on vacation without its user ever realizing that this has happened.

To be sure, criminals are not trying to steal the device. Rather, they want the attorney to continue to use it because the malware will enable them to capture passwords and other confidential information. More importantly, should it be connected to work systems or email, they, too, can become infected with the malware.

Similarly, if a work device is connected to a home network, when a personal device infected with malware connects to that network it can potentially infect the work device. And when the work device is connected to a law firm's systems, they also may be infected.

What all of this points to is that, until individual attorneys are much more vigilant about their personal cybersecurity, they are the weakest link in their firms' cyberdefenses. And their employers may be wasting a lot of money on upgrading their protections.

However, there are some steps that attorneys can take to reduce the risks that they create for their employers. To be sure, at some point everyone will be breached. However, following these commonsense rules and principles will reduce both the frequency of such occurrences and the potential resulting damage.

1. Use unique, lengthy, alphanumeric passwords for each online account.

There are large cybergangs operating in countries such as China, Russia, Iran and North Korea that have developed sophisticated tactics using computers for correctly guessing passwords. Information gathered from corporate data breaches as well as unprotected personal online information are fed into algorithms that generate thousands of variations of passwords. The passwords are used to try and breach the online accounts associated with an individual's email addresses.

These tactics compromise about 1 million passwords per week, in no small part because most people use relatively short, unsophisticated ones.[7]

For example, a recent study by Hive Systems showed that it took a computer model only

about two minutes to correctly guess an eight-character password made up of upper- and lowercase letters and numbers. Although an alphanumeric version — i.e., one with upper- and lowercase letters, numbers and symbols — of the password was stronger, the model correctly guessed it in only five minutes.

However, the same model would take 26 trillion years to correctly guess a randomly generated, 18-character alphanumeric password.[8]

2. Cyberprivacy is integral to cybersecurity.

Cybersecurity without cyberprivacy is ineffective. Thousands of online businesses regularly collect and sell immense amounts of personal information to third parties. Unfortunately, cybercriminals also can access the information and use it to identify and determine how to target potential victims.

Protecting cyberprivacy is uncomplicated. For starters, limit personal online information. Never post a photo or biography to any social medial accounts such as LinkedIn, Facebook, Instagram, etc. Likewise, provide only professional information on law firm sites. And only share an actual birthday online with governmental agencies as well as with airlines that must forward them to the Transportation Security Administration.

Additionally, most online companies effectively allow users to opt out of the collection and sharing of their information and limit those who can access it. However, because they make a great deal of money from selling data, they make doing so burdensome. It requires navigating a maze of multiple webpages to determine which settings to turn on for each account.

Similarly, it is also important to engage a host of privacy settings on devices, search engines and web browsers.

Lastly, engaging these settings is not a one-time event. Rather, online companies regularly change them, making it essential to review and update them at least annually.

3. Take advantage of security settings on devices and online accounts

Most devices and online accounts include security features that few users utilize. When engaged, they make it much harder to hack either, and they also limit the information lost in a breach.

For example, many devices and web browsers automatically record the passwords for every online account that they access. Hence, if the device is breached, every online account that it has accessed is likewise compromised. But there are both device and browser settings that if engaged prevent it from recording this information.

Similarly, hackers often target devices when they are being backed up to the cloud on home networks or public Wi-Fi. Certain devices offer end-to-end encryption capabilities that, when engaged, encrypt data being sent to the cloud and prevent hackers from being able to access it in transit.

Many online accounts offer multifactor authentication. When it is engaged, it requires users to provide multiple passcodes to access the account, thus preventing a breach should a password be compromised.

4. Avoid becoming an attractive target for cybercriminals.

Cybercriminals have limited time and resources and, thus, they prefer to go after potential victims who are easy to breach. These four steps make attorneys less attractive targets:

Minimize smart home technology.

Homes with smart technology — i.e., security cameras, digital lightbulbs, smart door locks and smart coffee pots, etc. — are particularly inviting to cybercriminals. This kind of technology is usually uncomplicated to hack, and one need only succeed with a single piece to compromise the entire home network, and everything connected to it.

Use USB blockers with rental cars and charging stations.

Cybercriminals can download data from devices that are plugged into automobiles or charging stations. They also can upload viruses to devices connected to the latter. A USB blocker is a low-cost — i.e., about $2 — prophylactic device that allows the device to charge while preventing the download of information or the upload of malware.

Wipe lost and retired devices.

Cybercriminals seek out previously used devices because they store information that can be used to steal assets or identities. Hence, whenever a device is lost or retired, it is critical to wipe its memory.

Provided one has engaged the necessary security settings and the lost device is connected online, remotely wiping it is uncomplicated. Retired devices that should be wiped include computers, smartphones, tablets and home assistants. However, as noted above, automobiles also download information, so before their lease expires or they are sold, they too need to be wiped.

Turn off Bluetooth when you are not using it.

Bluetooth is great technology that makes devices much more accessible. However, its downside is that it also allows anyone nearby to likewise access the device.

Cybercriminals regularly capitalize on this capability. For example, they look for someone on an airplane flight who is working on a laptop and is proximate, i.e., is within five or six rows. Unless the user has turned off the device's Bluetooth, criminals can look virtually into the device and steal information and passwords.

In conclusion, following these rules and principles reduces an attorney's likelihood of being breached and subsequently being used by cybercriminals to penetrate an employer's cyberdefenses.

As Robert Mueller, former director of the FBI, once pointed out, "There are only two types of companies: those that have been hacked and those that will be hacked."

Unless individual attorneys become more conscientious about their personal cybersecurity, they most certainly will have an opportunity to explain to their partners why their firm has joined the former.

Mark Hurley is chief executive officer of Digital Privacy & Protection LLC.

Carmine Cicalese is senior adviser and partner at the firm.

[1] https://arcticwolf.com/resources/blog/top-legal-industry-cyber-attacks/.

[2] https://cybernews.com/news/cadwalader-law-firm-hacked/.

[3] https://www.infosecurity-magazine.com/news/uber-data-exposed-law-firm-breach/, https://www.breachlock.com/resources/blog/uber-breach/#:~:text=Uber%20has%20experienced%20its%20third,their%20digital%20supply%20chain%20security.

[4] https://www.americanbar.org/groups/law_practice/publications/techreport/2022/.

[5] https://www.americanbar.org/news/abanews/aba-news-archives/2022/09/aba-survey-lawyers-remote-work/.

[6] https://www.wsj.com/articles/apple-iphone-security-theft-passcode-data-privacya-basic-iphone-feature-helps-criminals-steal-your-digital-life-cbf14b1a, https://appleinsider.com/articles/23/02/24/if-both-your-iphone-and-passcode-get-stolen-youre-in-deep-trouble.

[7] https://www.secplicity.org/2021/05/04/2021-world-password-day-how-many-will-be-stolen-this-year/.

[8] https://www.hivesystems.io/blog/are-your-passwords-in-the-green.