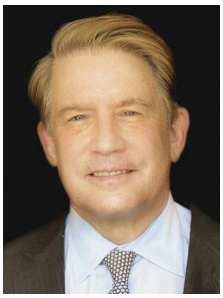
Law Firms Cannot Ignore Attorneys' Personal Cybersecurity

By **Mark Hurley and Carmine Cicalese** (July 20, 2023)



Mark Hurley

Carmine Cicalese

Most law firms recognize that cybersecurity risks are an existential threat to both their clients and their own financial well-being.

This is unsurprising given more than 750,000 Americans have had personal information compromised in law firm breaches since 2020,[1] resulting in lost business, embarrassment and lawsuits for many organizations.

Additionally, attorneys have long had an ethical duty under Rule 106(c) of the American Bar Association's Model Rules of Professional Conduct to make reasonable efforts to protect client information. Unsurprisingly, many firms have spent millions of dollars upgrading their cyberdefenses.

However, cybersecurity is an exercise in risk minimization, not elimination. It involves layers of defense, each focused on the many different points in which humans interact with technology.

The first layers of law firm cyberdefenses typically address how their attorneys and employees interact with systems when they are working for their clients. Unfortunately, cybercriminals are quite adept at adapting their tactics and identifying weak links and gaps.

Lax personal cybersecurity by attorneys creates numerous opportunities for breaching their employers' systems. Indeed, targeting lawyers away from work, at home and on vacation provides a far easier path for hacking a law firm than a direct cyberattack.

Ignoring this threat not only increases the likelihood of a breach and the theft of sensitive client information, it also may be a violation of ethical duties.

More specifically, Rule 106(c) also applies to attorneys when they are not at the office, and in 2017, the ABA published Formal Opinion 477R, which provides a nonexhaustive list of factors for determining what constitutes reasonable efforts in cybersecurity including:

- Sensitivity of the information,
- Likelihood of disclosure if additional safeguards are not employed,
- Cost of employing additional safeguards,
- Difficulty of implementing the safeguards, and

- Extent to which the safeguards adversely affect the lawyer's ability to represent clients.[2]

For law firms, taking the necessary steps to ensure that attorneys operate safely online away from work significantly lowers the likelihood of a breach and, thus, the theft of sensitive information.

Moreover, the steps required are both relatively uncomplicated and inexpensive to implement. And doing them in no way adversely affects a lawyer's ability to represent clients.

In other words, organizations that ignore their attorneys' personal cybersecurity are not using their best efforts to protect client information, painting a target on the organization's back, and simplifying the job of plaintiffs attorneys if the organization is breached and has sensitive client information stolen.

And candidly, it is not a question of "if" but of "when." Five class action lawsuits have already been filed in 2023 related to such breaches.[3]

It is also far more challenging to defend against such a suit if the defendant has disregarded a clear, published and accepted set of industrywide duties and standards for protecting client information.

Far more problematic, an organization may find that it effectively is uninsured against any resulting court-ordered judgment because cyberinsurance policies increasingly now include a specific exclusion for employee error.[4] It is unclear how any firm could credibly take the position that a breach caused by its attorneys being irresponsible about their personal cybersecurity would not fall under this exclusion.

More succinctly, how attorneys operate online away from work creates a potential moral hazard for their employers that is foolish to ignore. Although the attorney causing the breach might be terminated, the firm's partners could lose millions of dollars.

The good news is that it is relatively uncomplicated for law firms to ensure that their attorneys are more responsible when personally operating online. The necessary steps are merely an extension of what smart law firm chief information security officers already have implemented for their organizations.

More specifically, they have created secure systems to which only company-owned and managed devices can connect, the devices have been locked down by engaging security and privacy settings, and each employee's work online accounts use randomly generated unique 20-digit alphanumeric passwords that are stored in a password manager. And when using work devices online, attorneys now are required to encrypt their traffic using a virtual private network.

Law firms should take similar steps with their attorneys' personal devices and home networks to ensure that they operate safely online away from work. Every device that connects to their home networks should be locked down, their personal online accounts protected by unique, sophisticated passwords that should be stored in a personal password manager, and they should use a VPN whenever they are online.

The only substantive additional step required involves protecting cyberprivacy by engaging the necessary settings on online accounts, web browsers and search engines. Doing so makes it much harder for cybercriminals to target and victimize attorneys away from work.

It also prevents downloading videos from unprotected personal social media accounts that can be used along with artificial intelligence software to clone both voices and images. Criminals regularly do this so they can pose as an employee of an organization in both online video and telephonic communications.

The primary limitation on the ability of law firms to create this additional layer of cyber protection is the necessary information technology staffing. Most lawyers and their families have multiple personal devices and online accounts and unless one addresses cybersecurity and cyberprivacy for an entire household, it creates gaps that cybercriminals can easily potentially exploit.

Consequently, current law firm IT staff would have to be significantly expanded to help oversee as many as five to 10 times more devices and online accounts than they do now.

Alternatively, many industry participants already use contract IT workers for certain tasks. They could similarly use ones with experience and expertise in cybersecurity to help handle the larger workload.

Regardless, law firms cannot continue to ignore their attorneys' personal online behavior. The potential cost is simply too great.

Mark Hurley is the CEO and Carmine Cicalese is a senior adviser and partner at Digital Privacy and Protection.

[1] https://www.law.com/americanlawyer/2023/01/10/cyberattacks-inevitable-for-law-firms-highlighting-need-for-comprehensive-incident-response-plans/#:~:text=Law%20Firm%20Data%20Breaches%20Exploded%20Since%202020&text=In%202020%2C%20law%20firm%20data,data%20was%20compromised%20in%202021.

[2] https://www.americanbar.org/news/abanews/publications/youraba/2017/june-2017/aba-formal-opinion-477r--securing-communication-of-protected-cli/.

[3]https://www.bloomberglaw.com/login?target=https%3A%2F%2Fwww.bloomberglaw.com%2Fproduct%2Fblaw%2Fbloomberglawnews%2Fbusiness-and-practice%2FBNA%2000000189-0dc6-d67c-a3ff-1df6caff0001%3FisAlert%3Dfalse.

[4] https://www.tripwire.com/state-of-security/changing-dynamics-cyber-insurance.