Why Are Lawyers So Terrible at Cybersecurity?

by Sharon D. Nelson, Esq., John W. Simek, and Michael C. Maschke

Let Us Count the Ways in Which Lawyers Are Terrible at Cybersecurity – and Then Talk About the New ABA Resolution on Cybersecurity

It is absolutely true that we tear our hair out (figuratively) when we attempt to give law firms good cybersecurity solutions at a modest price and they decline. Mind you, they know that we have seen a significant rise in law firm data breaches in 2023. The headlines are everywhere. The gnashing of teeth by law firm managing partners is legendary and evident in all the headlines.

"Too expensive" is the first reaction. We constantly wonder if they understand how expensive a data breach is. "We're not a target" is the second reaction. That comes mostly from the smaller firms – who have not apparently observed that small/midsize firms are being attacked with vigor.

"It's too disruptive to our operations" is often heard. Had they ever observed the disruption of a data breach, they might understand that true disruption to law firm operations is possible.

One of the classic reactions is "we have cyberinsurance." While having cyberinsurance is a very good thing, it is not going to help a law firm whose data has been taken. And many cyberinsurance companies have strict policies about security measures the firm must take just to be covered – we can't tell you how many times they have affirmed, for instance, that they use multi-factor authentication (MA) everywhere. Their noses are longer than Pinocchio's. And that's only one example of commonly misrepresenting the firm's security posture. Guess what? If your answers to a cyberinsurance company's questionnaire are not truthful, you may not have the insurance coverage you thought you had.

The American Bar Association Adopts Resolution 609 at its August Annual Meeting

We were glad to see the ABA Adopt Resolution 609 in August 2023. It was sorely needed.

We loved the words of Ruth Hill Bro, a special adviser to the ABA Cybersecurity Task Force (which author Nelson served on for a number of years): "Cybersecurity is a journey, and you never really arrive."

Well put. Our own mantra is "there is no set it and forget it in cybersecurity." More than ever, this is true in a time when Generative AI is causing consternation with its ability to produce (as one example) phishing emails without any of the usual tell-tale signs that they are phishing emails. They get the grammar and spelling right, they use real-life logos and they may even corrupt otherwise "good AI" to be bad. The "tricks of the trade" at corrupting AI are spreading across the internet like wildfire.

The Essence of ABA Resolution 609

It may not be entirely new, but for the first time, artificial intelligence has made an appearance, as well it should. The best way to give readers useful information is to quote the essence of the resolution directly:

"RESOLVED, That the American Bar Association urges all lawyers to keep informed about new and emerging technologies and protect digital products, systems, and data (including Artificial Intelligence and Machine Learning) from unauthorized access, use, and modification;

FURTHER RESOLVED, that the American Bar Association urges lawyers to enhance their cybersecurity and infrastructure to protect confidential client information and to keep clients informed;

FURTHER RESOLVED, That the American Bar Association urges lawyers and law firms to conduct cybersecurity due diligence regarding third-party and vendor products and services;

FURTHER RESOLVED, That the American Bar Association urges lawyers to advise clients, on their legal duty to raise the level of their own cybersecurity measures;

FURTHER RESOLVED, That the American Bar Association urges lawyers and law practices to incorporate cybersecurity and emerging technologies into their education and training programs; and

FURTHER RESOLVED, That the American Bar Association urges lawyers and law practices to enhance cybersecurity through a diverse and technologically competent workforce."

Most of this is an updated restatement of what has gone before, but the updates were sorely needed. Get a cup of coffee, read the resolution again and take note of what you are NOT doing in your firm.

ABA Also Adopts Guides for AI

At the August meeting, the ABA also adopted Resolution 604, which contains guidance for the use of artificial intelligence. Some time back, the ABA had adopted resolutions about AI and the legal profession. However, Resolution 604 encompasses principles for the design, development and deployment of AI by technology organizations.

As we have often said, "The greed of the tech titans may pave the road to Skynet."

Apparently, we are not alone in worrying about the future of AI.

Resolution 604 states that AI developers should ensure their products are subject to human authority, oversight and control, include accountability measures if developers have not taken reasonable steps to mitigate harm or injury; and provide transparency and traceability for their products.

A noble attempt to formulate good guidelines, but where is the enforceability? And AI developers have a strong motivation (the obscene amounts of money they are raking in) to make their AI a black box (you don't know how it works, in simple terms).

What this means for lawyers who use AI is not currently clear. How can lawyers be ethically competent with the technology of AI if they don't know how it works?

ABA Forms Task Force on Law and Artificial Intelligence

We learned on August 28 that the ABA has formed the ABA Task Force on Law and Artificial Intelligence to analyze how AI will impact the legal profession and to discuss the new ethical questions that the technology will raise for lawyers.

The ABA is going about this the right way. There are seven "special advisors" to the new task force. They include former U.S. Homeland Security Secretary Michael Chertoff and Seth Waxman, a former U.S. Solicitor General.

Other advisors include former U.S. Patent and Trademark Office director Michelle Lee and former U.S. Department of Homeland Security general counsel Ivan Fong. The group will be chaired by Lucy Thomson, a Washington D.C. based lawyer and security engineer. Some heavy hitters there!

We are truly glad to see that the furiously fast adoption of generative AI has resulted in a coalition of many people who want to put guardrails around a technology that is so potentially dangerous and impactful. Lawyers certainly need ethical guidance on this new technology.

Final Words

To quote our good friend Ed Walters, founder of Fastcase and now the Chief Strategy Officer of vLex, "The most important question when working with AI is 'what could possibly go wrong?'"

The answer, as we have already seen, is "a lot."

Sharon D. Nelson *is a practicing attorney and the 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 ABA.* *snelson@senseient.com*

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm.* *jsimek@senseient.com*

Michael C. Maschke *is the CEO/Director of Cybersecurity and Digital Forensics of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional.* *mmaschke@senseient.com*