

BY UMER M. SIDDIQUI

AI's Sharp Edges

A lawyer's cybersecurity obligations regarding generative artificial intelligence.



▲
UMER M. SIDDIQUI is a former digital forensics analyst, now a senior associate at Wood Smith Henning & Berman, providing counsel to clients regarding cybersecurity issues, including generative artificial intelligence.

umer.siddiqui7@gmail.com

“ALWAYS STAY CURRENT WITH technology but be wary of the bleeding edge—it’s sharp.”

My old chief information security officer told me that, back when I was a young digital forensics analyst at Motorola. Years later, and now as an associate, I see the truth in that. It’s no surprise that with the rise of generative artificial intelligence (AI), the world stands changed. For the legal profession, we are not immune from the allure of this new technology. Slowly, yet surely, we’re being drawn to the edge.

With the ubiquitous use of AI, lawyers must recall their duty to protect the confidentiality and privacy of their clients, be aware of the complexity of any new technology they hope to harness, and take reasonable steps to educate themselves on cybersecurity risks inherent in the use of this technology. AI products can quicken our research, analyze our data, and automate simple but time-consuming tasks. But they also can place the confidentiality and privacy of our clients’ data at risk.

Another reason lawyers must become familiar with AI is to better ward off cybercriminals, who also are using AI in their cyberattacks against organizations big and small. To serve our clients better, and to maintain the confidentiality and privacy of our client data, we can no longer remain content to let others handle the technology under the hood. The change is not coming; it is already here. To work and thrive in this new technological world, attorneys must become increasingly capable with this fundamental technology and understand how to protect client data.

This article will examine the convergence of a lawyer’s responsibility toward AI and cybersecurity. It will explore our role as custodians of highly sensitive client information and the fraught technological environment we face, and it will offer advice on how to navigate this brave new world.

The evolving cybersecurity landscape

Like most businesses in the U.S., many law firms are adopting AI into their work environments. But few articles speak to the salient threats that exist when employing AI at work, namely: the cybersecurity issues inherent in the use of AI and the cybersecurity issues being proliferated by threat actors using AI. Both shall be addressed in turn.

Inherent AI risks

Most attorneys know by now that client data should not be entered into free versions of AI platforms such as OpenAI’s ChatGPT, Microsoft’s Copilot, DeepSeek, and others, since it

TAKEAWAYS >>

- While attorneys are putting artificial intelligence (AI) to great use, they remain obligated to deeply understand the technology and its weaknesses.

- Law firms, both big and small, must view cybersecurity as a strategic investment in client service and professionalism.

- All attorneys must:
 - 1) understand how cybercriminals use AI to launch sophisticated attacks; and
 - 2) take reasonable, appropriate measures to mitigate those risks.

WITH THE UBIQUITOUS USE OF AI, LAWYERS MUST RECALL THEIR DUTY TO PROTECT THE CONFIDENTIALITY AND PRIVACY OF THEIR CLIENTS, BE AWARE OF THE COMPLEXITY OF ANY NEW TECHNOLOGY THEY HOPE TO HARNESS, AND TAKE REASONABLE STEPS TO EDUCATE THEMSELVES ON CYBERSECURITY RISKS INHERENT IN THE USE OF THIS TECHNOLOGY.

would breach the confidentiality of client data. Information given to these platforms is, by default, used to further train them, which improperly exposes sensitive client data.

But even using private AI systems carries risks. According to reports, code that organizations create with AI is alarmingly insecure. Nearly 45 percent of code samples generated by large language AI models failed security tests and even introduced top security vulnerabilities into their code.¹

Also, AI chatbots, whether free or used with a subscription, are not immune from spreading incorrect information. “AI chatbots are getting dramatically worse at spreading falsehoods”² Because AI is still capable of producing hallucinations,³ attorneys need to be cautious when using anything produced by AI or leveraging its features. For example, Amazon scrapped an AI tool intended to be used for hiring when it found it discriminated against women,⁴ which could have opened it up to legal liability. Users of the coding software for the company Cursor faced a similar issue. When a user noticed strange behavior while using Cursor’s software, the user contacted Cursor support. An AI agent told them that the strange behavior was expected under a new policy. But no such policy existed. The AI model made the policy up, sparking a wave of complaints and cancellation threats.⁵ The assertion of a make-believe policy along

ISBA RESOURCES >>

- Ed Finkel, *What’s in Your Retainer?*, 113 Ill. B.J. 18 (Apr. 2025), law.isba.org/4kTpqM7.
- ISBA Practice HQ, *Questions to Ask Your AI Provider*, law.isba.org/4wx7XzO.
- ISBA Practice HQ, *Vetting AI for Attorneys*, law.isba.org/3NCMGAf.

with any harm received by users could expose the company to compounded risk.

Risks from external threat actors

The rise of AI has only accelerated many of the same cybersecurity threats that have plagued law firms for years. Empowered by AI, these attacks have become increasingly costly. The “[a]verage breach costs in the United States reached a record USD 10.22 million, a 9 percent increase over last year, driven in part by higher regulatory fines and detection and escalation costs.”⁶ For small- and medium-sized businesses, the cost of a data breach can easily skyrocket into the hundreds of thousands of dollars after legal costs, forensics, and remediation efforts—to say nothing of any enforcement penalty.

The legal sector has become an especially attractive target because even small firms routinely handle highly sensitive client data, including personally identifiable information, trade secrets, and other confidential matters that can be extremely valuable to criminal elements.

While AI has been used to make our lives as attorneys easier and provide more capable and competent representation for our clients, it is helpful to understand some of the most common and deceptive means by which AI can be used against us.

Phishing on steroids. According to reports, since ChatGPT was released in 2022, phishing attacks have increased by 4,151 percent, representing a severe escalation in cyberthreat activity.⁷ The same technology used to help us draft our legal documents is now being used to create ever more believable phishing attacks, making these attacks more personalized and urgent.

Social engineering has emerged as the dominant threat facing the legal profession, accounting for nearly 40 percent of all data breaches.⁸ And 20 percent of these social engineering attacks use “pretexting,”⁹ where threat actors use believable scenarios (a pretext) to gain a victim’s trust and trick them into divulging sensitive information or granting access to sensitive systems.

Despite AI advancements, human-centric attacks remain the most common method of gaining unauthorized access to sensitive data.

Thanks to AI ..., phishing attacks are skyrocketing—phishing surged ... in late 2024, and over 80 percent of phishing emails now incorporate AI, with nearly 80 percent of recipients opening them. These messages are bypassing filters and fooling employees.¹⁰

Consider how often firms handle significant funds that must be used to serve clients’ needs. The fast-paced nature

1. Jens Wessling, *We Asked 100+ AI Models to Write Code. Here’s How Many Failed Security Tests*, VeraCode (July 30, 2025), law.isba.org/4gZGh1J.

2. Emma Woollacott, *AI Chatbots Are Feeding You More False Information Than Ever*, Forbes (Sept. 5, 2025), law.isba.org/4fxFcqv.

3. A hallucination is where a large language model “perceives” patterns or objects that are nonexistent in its data, creating outputs that are nonsensical or otherwise factually incorrect.

4. Jeffrey Dastin, *Insight—Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*, Reuters (Oct. 10, 2018), law.isba.org/4fVSe7w.

5. Benj Edwards, *An AI Customer Service Chatbot Made Up a Company Policy—and Created a Mess*, Wired (Apr. 19, 2025), law.isba.org/4vUqaGt.

6. IBM, 2025 Cost of a Data Breach Report: the AI Oversight Gap, at 11.

7. Kasey Babcock, *AI Phishing Attacks Are on the Rise—Are You Prepared?*, bitwarden (July 15, 2025), law.isba.org/4x2TThf.

8. Verizon, 2024 Data Breach Investigations Report, at 69.

9. *Id.*

10. Joseph J. Lazzarotti, *The Growing Cyber Risks From AI—and How Organizations Can Fight Back*, National Law Review (June 16, 2025), law.isba.org/4gVK6F5.

of litigation requires quick decision-making and actions. Supply chain, payroll, and human resource departments often establish trusted relationships and familiar contacts, all of which can be used to trick unsuspecting employees into divulging critical banking information or sensitive client data.

Ransomware. Ransomware relies on computer networks that are outdated and weakly defended. (In June 2026, the U.S. briefly forced Anthropic to disable new models due to their ability to spot security vulnerabilities.)

Ransomware attacks remain a significant threat to a law firm's security, accounting for roughly 33 percent of all data breaches and representing the top threat among 92 percent of industries.¹¹ And while ransomware payments have decreased, they are still hovering around half a million dollars, indicating that these attacks remain financially devastating for victims.¹²

Ransomware attacks can potentially drive businesses into insolvency. When ransomware encrypts essential case files or client documents, law firms face the impossible choice between paying exorbitant ransom demands or potentially violating their duties and ethical obligations to clients.

Voice cloning. Voice cloning has become the new frontier of deception against law firms and businesses. According to cyberdefense experts McAfee, it only takes three seconds for AI to create a convincing representation of a person's voice.¹³ These attacks have become increasingly effective as AI can convincingly emulate a person's voice, unique intonation, rhythm, and lilt.

The costs of such scams are growing rapidly. "Of the people who reported losing money, 36 percent said they lost between \$500 and \$3,000, while 7 percent got taken for sums anywhere between \$5,000 and \$15,000."¹⁴ These attacks are usually paired with high-pressure "spear-phishing"¹⁵ campaigns. A late-night call, seemingly from a partner ("it sounded just like her"), could be a threat actor trying to gain access

to your law firm's restricted data.

Deepfakes. As with voice cloning, deepfake videos are growing in sophistication and complexity. "Financial losses from deepfake-enabled fraud exceeded \$200 million during the first quarter of 2025, according to Resemble AI's Q1 2025 Deepfake Incident Report"¹⁶ This figure represents only the beginning of what experts predict will become a dominant threat vector in the cybercrime landscape. Deepfake technology poses risks to attorneys because it can affect our ability to litigate:

In the courtroom context, deepfakes will impact evidence authenticity, witness credibility, and the integrity of the judicial process, not only because of deepfakes themselves but also because genuine evidence now can be alleged to be false, requiring this to be disproven.¹⁷

The ethical and professional imperative

Attorneys are bound to adhere to the Illinois Rules of Professional Conduct (IRPC). In addition to the IRPC, the Illinois Supreme Court has published an AI policy for attorneys, judges, and court staff. The Illinois Attorney Registration and Disciplinary Commission also has released extensive guidelines on the use of AI.¹⁸ But reliance on the IRPC is the common thread throughout all of these sources.

Illinois Rule of Professional Conduct 1.1. Competence.

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology¹⁹

Rule 1.1 establishes the foundational duty of competence, requiring that lawyers provide competent representation that includes "the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." The Illinois Supreme Court's adoption of Comment 8 to Rule 1.1, effective Jan. 1, 2016, makes this obligation explicit regarding technology:²⁰

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant

THE LEGAL SECTOR HAS BECOME AN ESPECIALLY ATTRACTIVE TARGET BECAUSE EVEN SMALL FIRMS ROUTINELY HANDLE HIGHLY SENSITIVE CLIENT DATA, INCLUDING PERSONALLY IDENTIFIABLE INFORMATION, TRADE SECRETS, AND OTHER CONFIDENTIAL MATTERS THAT CAN BE EXTREMELY VALUABLE TO CRIMINAL ELEMENTS.

technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.²¹

For attorneys, this creates an affirmative duty to understand the opportunities and dangers that technology, including AI, presents to their practice. The Rule's intentionally broad language encompasses various aspects of legal technology, from email security and cloud storage risks to the growing use of AI tools in legal research and document preparation.

Illinois Rule of Professional Conduct 1.6. Confidentiality. A fundamental Rule of our practice is that a lawyer:

11. Theodore J. Kobus III, Craig A. Hoffman & Lynn Sessions, *BakerHostetler Launches 2025 Data Security Incident Response Report*, BakerHostetler (Apr. 15, 2025), law.isba.org/45psUAF.

12. *Id.*

13. *AI Calling—Scammers Turn to AI Voice Cloning Tools for a New Breed of Scam*, McAfee (May 2025), law.isba.org/4wx5V7iL.

14. *Id.*

15. The act of attempting to fraudulently induce a specific target to reveal confidential information by impersonating a known or trusted sender.

16. Carolyn Giardina, *Deepfake-Enabled Fraud Has Already Caused \$200 Million in Financial Losses in 2025, New Report Finds*, Variety (Apr. 17, 2025), law.isba.org/4wq73oz.

17. George Bellas, *Deepfakes in the Courtroom: Problems and Solutions*, Trial Briefs, Jan. 2025, law.isba.org/4yMoQbg.

18. See Ill. Sup. Ct., Policy on Artificial Intelligence (eff. Jan. 1, 2025), law.isba.org/ILSupCt_AI. See also, Attorney Registration and Disciplinary Commission, The Illinois Attorney's Guide to Implementing AI (2025), law.isba.org/47WyeE63.

19. Ill. R. Pro. Conduct R. 1.1.

20. Robert Ambrogi, *Illinois Adopts Duty of Technology Competence; Is Now 15th State to Do So*, LawSites (Oct. 16, 2015), law.isba.org/4fq6pBH.

21. *Illinois Attorneys Have a Duty of Technological Competence*, Segal McCambridge (Jan. 1, 2016), law.isba.org/4fdhpkL.

shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.²²

Furthermore:

Paragraph (e) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (e) if the lawyer has made reasonable efforts to prevent the access or disclosure.

Paragraph (e) emphasizes that unauthorized access or disclosure does not constitute a violation "if the lawyer has made reasonable efforts to prevent the access or disclosure," further establishing the need for lawyers to take a continuous approach to safeguarding client data.

ABA Formal Opinion 483. Issued in October 2018, the opinion establishes comprehensive guidance for lawyers' obligations both before and after cyber incidents occur. It emphasizes that ABA Model Rule 1.1's competence requirement includes understanding cybersecurity technologies and implementing reasonable security measures.²³

ABA Formal Opinion 512. Released in July 2024, this opinion offers a comprehensive ethical framework for the use of AI. The opinion clarifies that: to competently use an [AI] tool in a client representation, lawyers need not become [AI] experts. Rather, lawyers must have a reasonable understanding of the capabilities and limitations of the specific [AI] technology that the lawyer might use.²⁴

The opinion emphasizes that understanding AI's capabilities and limitations must be an ongoing practice: This means that lawyers should either

acquire a reasonable understanding of the benefits and risks of the [AI] tools that they employ in their practices or draw on the expertise of others who can provide guidance about the relevant [AI] tool's capabilities and limitations. This is not a static undertaking.²⁵

Mitigating AI-driven cyberthreats

Attorneys and their employees can take several steps to leverage AI safely and securely.

Focus on people. The human element remains the most critical factor in cybersecurity defense, even as AI transforms the threat landscape. Organizations with comprehensive employee training programs reduce breach costs by an average of \$232,867,²⁶ making security education one of the highest-return investments law firms can make.

Technical infrastructure hardening. Multifactor authentication (MFA) can prevent 99.9 percent of attacks on accounts,²⁷ making it an essential security control for every law firm regardless of size. Modern MFA implementations should go beyond simple SMS codes to include app-based authentication, hardware tokens, and biometric verification methods that are more resistant to AI-enhanced social engineering attacks.

Law firms should implement comprehensive endpoint protection that includes AI-powered threat-detection capabilities. These systems can identify unusual patterns of behavior that may indicate compromise, including subtle signs of social engineering attacks or unauthorized access attempts that human monitoring might miss.

Incident response planning. Less than one-third of small and medium-sized organizations currently have an incident-response plan in place, despite the critical importance of rapid response in minimizing breach damage. For law firms, incident-response planning is not just a best practice; it's an ethical obligation

under IRPC 1.1 and 1.6.

Law firms must view cybersecurity as a strategic investment in client service and professional competence. The cost of implementing comprehensive security measures is minimal compared to the potential costs of a data breach, which can include financial losses, regulatory fines, professional discipline, and permanent reputational damage. Cyber insurance can play a critical role in supporting an organization's efforts to insulate itself from the harm of a cyber incident.

Check and double-check your work. While AI chatbots and other research tools can save time, a human must validate everything AI produces. Citations, especially, should be rigorously scrutinized when presenting any written work before any court or tribunal.

Conclusion

The intersection of generative AI and cybersecurity creates unprecedented opportunities and threats for the legal profession. As custodians of highly sensitive client information and essential participants in the justice system, lawyers cannot afford to ignore these rapidly evolving challenges.

Attorneys must recognize that cybersecurity in the age of AI requires ongoing attention, continuous learning, and adaptive responses to new and emerging threats. The firms that will thrive are those that embrace cybersecurity as a core strategy, not only to protect their clients, but to lead by example in shaping a more resilient legal profession. **EB**

22. Ill. R. Pro. Conduct R. 1.6.

23. A.B.A. Comm. on Ethics & Pro. Resp., Formal Op. 483, at 9 (2018).

24. A.B.A. Comm. on Ethics & Pro. Resp., Formal Op. 512, at 3 (2024).

25. *Id.*

26. IBM, 2023 Cost of a Data Breach Report, at 28.

27. Multifactor Authentication, Cybersecurity & Infrastructure Security Agency, law.isba.org/4bariOM (last visited July 14, 2026).