| SERVING CHICAGO'S LEGAL COMMUNITY FOR 164 YEARS |

Chicago Daily Law Bulletin®

VOLUME 168, NO. 116

LAW BULLETIN MEDIA

A primer on technology competence for Illinois attorneys includes ethics

LEGAL TECH

F. KEITH BROWN and MICHAEL KOSS

F. KEITH BROWN *is senior mediator and arbitrator at ADR Systems.* MICHAEL KOSS *is ADR Systems' business development and marketing assistant manager.*

Whether attorneys are engaged in alternative dispute resolution or litigation, they must leverage technology in new ways to be efficient and effective in their practice. With the onset of remote mediation, arbitration and court proceedings, technological proficiency is even more important for competent representation.

There is no standard set of technology competencies for attorneys, as noted by recent scholarship, and only a few states require technology training as a component of continuing legal education.

What, then, is the litmus test for a technologically competent attorney?

An Illinois-licensed attorney can find some guidance from various ethical opinions. Here, in part 1 of 2, you will learn what technology competency means in an evolving legal landscape by reviewing topics regarding personal security, third-party vendors and cloud-based services.

Personal security

Technology competence begins with personal security. An attorney's individual, daily security practices are linchpins for wider organizational security — even more so while working remotely. Using personal devices for professional work may pose security risks if mismanaged. Relatedly, bad actors can unleash a slew of surreptitious threats — malware, ransomware, phishing scams, email spoofing and typo-squatting threats, among many others — to extract money and confidential information from a law firm. Each of these threats can begin at the individual level but spiral into more systemic, costly problems.

Luckily, basic security practices can help circumvent many technology-related threats:

• Access the internet via a secure, private wi-fi connection or virtual private network (VPN).

• Avoid public wi-fi networks.

• Use sophisticated, non-personal passwords with unique characters and multi-factor authentication to enter firm systems and work accounts (if not implemented by a contracted or in-house information technology provider).

• Implement firewall, antivirus software and data-encryption tools on work or personal devices used to access work-related accounts.

• Back up stores of data in the event of data loss or breach — say, through an external hard drive — or confirm that cloud-based services do so already.

• Consistently update communication and operational software to patch security gaps, bringing them up to date with improvements made by the software provider.

These recommendations are paraphrased from the ABA's Formal Opinion on virtual practice, which was published as a general roadmap for practicing law responsibly from remote locations.

The opinion is not exhaustive, however. Counsel can also practice technological due diligence in more rudimentary, manual ways:

• Convey any login information via private and encrypted channels.

• Send sensitive documents to off-server recipients with password protections or via vetted file-sharing tools.

• Remove client information from unmanaged file storage services.

• Check the spelling of emails from suspicious or unfamiliar senders before clicking in-email links; this can thwart various social engineering and typo-squatting threats.

By practicing these recommendations, counsel can better mitigate cyberthreats that lick their chops at the prospect of troubling lawyers and law firms.

Third-party vendors, cloud-based services

Attorneys can engage third-party vendors and cloud-based services provided that they "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," as required by Rule 1.6 of the Illinois Supreme Court Rules of Professional Conduct and ABA Model Rules of Professional Conduct.

Here's the rub, however: While approximately 60% of attorneys utilize some type of cloud service (Dropbox being the most common), 35% of respondents to the ABA's 2021 Legal Technology Survey Report do not apply any of the ABA's standard cautionary cybersecurity measures, which include:

• Performing data back-ups.

• Securing socket layers (which secure communication via email, among other functions).

• Evaluating vendor company history.

• Reviewing terms of service.

• Checking ethical opinions.

• Negotiating confidentiality and legal service agreements with vendors.

Since attorneys may need to grant third-party vendors access to client information, they should ensure that such vendors, especially if non-legal in nature, "[have] in place or will institute reasonable procedures to safeguard the confidentiality of the client information." A written statement from the vendor regarding its "assurance of confidentiality" can minimize risk and liability for the attorneys soliciting such services.

Similar considerations apply when using cloud-based services. However, these platforms introduce a potential complication. They invariably store client data on separate, remote servers beyond counsel's direct control or access. Respondents to the recent ABA Legal Technology Survey Report on cloud computing listed control of data as a top concern about cloud services. While ethical opinions do not offer a procedure that counsel must follow when selecting a cloud-based service, the ISBA offers suggestions for counsel when performing a "due diligence investigation." Some of these suggestions include:

• Assessing a provider's security precautions to protect client information, including firewalls, password protections and encryption.

• Establishing an agreement that ensures that the provider will abide by counsel's duties of confidentiality and will alert counsel of any breaches or requests for client information.

• Requiring that all data be backed up and retrievable by counsel.

• Reviewing the terms of service for their hardware devices and software systems and future updates to those to terms.

It is particularly helpful for counsel to understand the ethical obligations involving third-party vendors and cloud-based services so they can effectively vet prospective technology tools from the outset. While many vendors may comply with counsel's ethical obligations — and especially case and practice management tools designed for attorneys — it is unwise to simply assume that is the case.

Technology competency goes beyond personal security, third-party vendors and cloud-based services, however. In part 2, we will address an ever more important aspect of technology competency for attorneys: responding to data breaches and cyberattacks.

| SERVING CHICAGO'S LEGAL COMMUNITY FOR 164 YEARS |

Chicago Daily Law Bulletin®

VOLUME 168, NO. 116

LAW BULLETIN MEDIA

How attorneys should respond amid increasing data breaches, cyberattacks

LEGAL TECH

F. KEITH BROWN and MICHAEL KOSS

F. KEITH BROWN *is senior mediator and arbitrator at ADR Systems.* MICHAEL KOSS *is ADR Systems' business development and marketing assistant manager.*

We presented an overview last week of what technology competency means in an evolving legal landscape by reviewing topics regarding personal security, third-party vendors and cloud-based services. Now we will address an ever more important aspect of technology competency for attorneys: responding to data breaches and cyberattacks.

Cyberattacks increased by approximately 50% per week for corporate networks in 2021 versus 2020 — itself a record-breaking year of increased malicious emails. The unfortunate reality is that cyberattacks really are an inevitable risk, as others have already underscored.

The average cost of a data breach can be severe: $4.24 million — and even more for a ransomware attack, which commonly target law firms — paid out in any combination of legal fees, fines, forensic analysis, hardware and software replacement, and lost revenue and reputation.

The ABA's Formal Opinion 483 out-lines counsels' obligations to monitor for data breaches and cyber incidents, restore systems, determine what occurred, notify current and former clients of the incident in a timely man-ner and explain how they or their firm intends to recover confidential client information. In short, counsel must minimize threats and maximize the response to them.

Incident response plans are crucial to that effort. They should enumerate how counsel will monitor a law firm's internet-connected devices, data sources, and third-party and cloud-based vendors, as well as how counsel will protect a law firm's systems from the effects of security threats. The SANS Institute has developed a six-step incident response process that counsel can reference to suit the cybersecurity needs of their firm.

Ethical obligations can dovetail with statutory ones. Counsel trusted with protected personal health information must comply with Health Insurance Portability and Accountability Act guidelines or other federal safety measures. Covered entities and business associates must safeguard against the threat of cyber incidents and ensure the same of subcontractors.

Likewise, counsel may need to conform client communications to state data breach law guidelines and certain foreign regulations. Illinois' Personal Information Protection Act (815 ILCS 530/) generally requires that communications be sent out expediently to Illinois residents whose "personal data" — Social Security numbers, driver's licenses, debit and credit card numbers, insurance information, certain biometric information and log-in credentials — was breached. Counsel must provide toll-free contact information for consumer reporting agencies and the Federal Trade Commission in these communications, and they must provide information regarding what entities to contact about fraud alerts or security freezes.

Relatedly, counsel that possess the personal data of clients from the European Union must comply with its General Data Protection Regulation (GDPR) guidelines on data security, protection, and breach notification, which can involve a narrow window of time to notify affected clients of a data breach.

Counsel's technology-related obligations to protect client information against cyberthreats is an imposing but manageable task — and one that is even more necessary today. Attorneys must stay abreast of innovation in the practice of law and continually increase their technological competence to serve their clients well. With careful attention to security practices, key ethical opinions, and relevant statutes, counsel can mitigate risks and better represent their clients in a milieu that is now more reliant on technology and remote interactions.