TIPS for Minimizing the Risk of a Law Firm Data Breach

BY KIRALYN LOCKE AND ARAM DESTEIAN

Lawyers are easy targets when it comes to two things – the first being jokes. For example, a man asks a lawyer, "Will you answer two questions for me if I give you $400?" The lawyer responds, "Yes. What is your second question?"

Not only are lawyers prime targets for jokes, but lawyers are also prime targets for cyberattacks. The question is not if a lawyer is going to be the target of a cyberattack, but when. Lawyers possess sensitive and valuable client information, including trade secrets, business strategies, and financial documents. In the eyes of a cybercriminal, that information equates to their next paycheck.

Under the Rules of Professional Conduct, lawyers have a duty to protect client data. This includes taking reasonable steps to mitigate the risk of cyber-attacks. While lawyers are not expected to be experts in all things cybersecurity, lawyers do need to have a basic understanding of how client information is stored and what steps must be taken to protect that information.

This duty differs based on what is reasonable under the circumstances. For example, if you work for a large, international law firm, it would be reasonable to have advanced security measures monitored and run by an in-house IT team. If you are a solo practitioner, you would not be expected to have these same resources available. This does not mean you are off the hook. Rather, no matter the size, a law firm is expected to have the infrastructure in place to protect client information. Recent guidance from the ABA has also provided that law firms of all sizes should have an incident response plan in place to protect against, detect and respond to cyberattacks.

The topic of how to protect against and respond to cyberattacks is far too detailed for a brief article. However, this article will provide basic suggestions for how a lawyer can protect client data. While it is impossible to completely erase the chances of falling victim to a cybercrime, these practical tips can help lesson those odds.

TIP 1 Do Not Connect to Public Wi-Fi

Lawyers sometimes have a difficult time "unplugging." Whether a lawyer is at a coffee shop down the street, or in a bistro across the ocean, the need to stay connected can feel obligatory. However, in certain circumstances, the only way to stay connected is by connecting to a public Wi-Fi network. While this is a convenient way to gain access to the internet, it can come with great risk.

Public Wi-Fi is vulnerable to takeovers by cybercriminals. If a cybercriminal gains control of or "spoofs" a public Wi-Fi network you connect to, you will be sending your information directly to the cybercriminal. Any information transmitted – emails, client information, credit card information, etc. – will be accessible to the cybercriminal.

A user generally has no way of knowing whether a public Wi-Fi network has been compromised. This is why the basic rule of thumb is: do not connect to a Wi-Fi network without taking steps to protect your information. If you need to connect to Wi-Fi, use a mobile hotspot, VPN,

or simply wait until you return to a Wi-Fi network you know is secure and trustworthy. This will help ensure that confidential client information is not intercepted.

TIP 2 Implement Multi-Factor Authentication

Multi-factor authentication, or MFA, is no longer a new concept. However, the legal field is notoriously slow for catching up with modern day trends in technology. If you are not currently using MFA to protect your data, the time to do so is now.

What is MFA? It is an added security measure which requires a user to verify their identify twice in order to access certain information. For example, entering your password on a computer is one form of verification. If you use MFA, perhaps you also receive a text that states, "are you trying to log in right now?" If you answer "yes," you gain access to your computer. If you answer "no," then anyone attempting to access your data is prevented from doing so. By using MFA, the risk of a data breach dramatically decreases.

There are plenty of programs and companies that can implement MFA for a lawyer or a law firm. While these services do come with a cost, the safety of client information (and protecting your license) is priceless.

TIP 3 Recognize Sophisticated Phishing Attacks

Most people are familiar with the concept of phishing attacks. Simply put, a phishing attack is a fraudulent communication that appears to be legitimate, intended to obtain information or money from the recipient. The sender of the communication is usually trying to convince the recipient to click a virus-filled link or provide sensitive information.

Traditional phishing attacks were easy to spot and sometimes even comical. For example, if an individual received an email from the Queen of Genovia requesting a Starbucks gift card, one would certainly recognize that as a scam. However, phishing attacks have become more sophisticated.

Nowadays, phishing attacks are specifically tailored toward the recipient. Because of this, these "fraudulent emails" have become more difficult to spot.

Consider the following scenario: A lawyer receives an email from JSmith@SmithLaw.com. This is not an email address that the lawyer recognizes, but the contents of the email appear to be legitimate. The email states, "Attached please find a link to the client documents in the pro bono matter your firm has agreed to assist on. Please let me know if you have any questions." The email contains a link to a well-known file sharing website. Once the link is clicked, the sender (a cybercriminal) gains access to the law firm's server and collects confidential client data.

The above scenario is a true example of a sophisticated phishing attack used on lawyers. While the email appears to be legitimate, it is not. This type of sophisticated phishing attack demonstrates the importance of exercising caution when receiving emails from unknown senders, even when the email appears to be safe.

Lawyers have an ethical duty to protect client data. This includes remaining vigilant about current cybersecurity threats and trends, and instituting policies and procedures to safeguard against the inadvertent disclosure of client information.

CONCLUSION

Lawyers have an ethical duty to protect client data. This includes remaining vigilant about current cybersecurity threats and trends, and instituting policies and procedures to safeguard against the inadvertent disclosure of client information. These practical pointers are just the tip of the iceberg intended to get you thinking about the importance of protecting client data.

While cyberattacks are not funny, sometimes lawyer jokes are. Here is a new joke to add to the never-ending list of lawyer jokes: What do you call a lawyer who ignores their ethical obligation to mitigate the risk of a cyber-attack? O-phish-ially in trouble.

Kiralyn Locke is an attorney with Bassford Remele. Kira focuses her practice in the areas of employment law, trust and estate litigation, and professional liability. She counsels her clients on how to navigate and prevent lawsuits. klocke@bassford.com, 612.376.1631. Aram Desteian is a shareholder with Bassford Remele. Aram represents businesses in complex commercial litigation and counsels and defends lawyers against professional liability claims, including lawsuits, investigations, board proceedings, and hearings involving legal ethics, legal malpractice, and other areas relating to the law of lawyering. Aram is chair of the MSBA professionalism and ethics section and serves as Bassford Remele's general counsel. adesteian@bassford.com, 612.746.1088.


ARAM DESTEIAN


KIRALYN LOCKE