Data Security and Professional Liability for Lawyers

As lawyers, we are often focused on the needs of our clients. Unfortunately, many lawyers never think about their own needs. While many of us may have helped a client deal with the fallout from a data breach, many lawyers are unprepared should such an event happen in their firm.

When you consider the information that law firms have in their possession, you begin to understand what makes them attractive targets to hackers. Patent information, trade secrets, insider information, even clients' personal information and Social Security numbers are stored on law firm servers. Law firms have access to a tremendous amount of sensitive information. The question is whether they are prepared for an attempted data breach and what ethical obligations they have to their clients to keep their data safe.

If you haven't given your clients' data security more than a passing thought, our Atlanta professional liability lawyer can help you understand the risk you face and what you must do to avoid an ethics complaint.

Your Ethical Obligations

Echoing Rule 1.6 of the ABA Model Rules, Section 1.6 of Georgia's Rules of Professional Conduct requires that lawyers keep clients' information confidential. And while it may be well-established that this obligation applies to inadvertent disclosures, the question is: How does this apply to a data breach where hackers are actively attempting to steal client information? In 2018, the ABA issued an advisory opinion that addresses this question.

Interestingly, the ABA opinion begins by focusing on an attorney's ethical obligation to provide competent representation to their clients (Model Rule and Georgia Rule 1.1). The ABA noted that in 2012 they opined that this duty of competence included a duty to understand any technology the attorney may use in the practice of law. The attorney's duty to understand can be accomplished through their own education or by hiring someone with the appropriate qualifications. Once understood, the attorney must use the technology in a way that protects the clients' confidential information. From there, the ABA opinion suggests that attorneys three potential ethical obligations pertaining specifically to data breaches:

1. **A duty to monitor**. The ABA concluded that lawyers must make reasonable efforts to continuously monitor their networks for security breaches. This includes an obligation to routinely assess their software, hardware, operating procedures and policies, and any plans for mitigating a data breach in the event that one should occur.
2. **A duty to stop the breach**. According to the ABA opinion, lawyers have an obligation to make reasonable efforts to stop any actual or suspected security breach and prevent further exposure of data. This may seem like common sense, but when coupled with the duty of competence, this also

requires that the law firm know how to stop a cyber attack.

3. **A duty to provide notice**. The ABA also concluded that lawyers have an ethical obligation to promptly inform their clients of the breach with sufficient information that they can make an informed decision. However, the ABA did not conclude that this obligation extends to former clients.

While the Georgia State Bar hasn't issued a similar opinion, it's safe to say that the ABA's opinion on the matter may be highly persuasive in the event of an ethical complaint. If nothing else, the ABA's opinion is highly informative - it identifies the ethical issues you must consider with respect to your clients' data.

Increased Risks and Challenges

Information technology has undergone a revolution in the last decade. Previously, data security consisted of keeping control of your paper files. In 2020, data security means managing personal smartphones, tablets, laptops, desktops, and network servers in addition to your paper files. Lawyers and staff may access your network remotely, communicate via text message and emails. Clients may have access via a dedicated portal. Hackers have recognized that the proliferation of IT access has led to multiple potential vulnerabilities, and they continue to exploit any weakness they can find. Without a doubt, protecting your clients' data may seem like an insurmountable obstacle.

Simple Steps You Can Take

As with any monumental task, breaking data security down into small, manageable objectives is an effective way to reach your goal. Here are some straightforward steps you can take to improve your firm's cybersecurity:

- **Staff up your IT department**. Many law firms consider any non-lawyers to be secondary citizens. When it comes to data security, you need to change your thinking. Your IT department is the only line of defense that you have against data breaches. Unfortunately, IT departments are often understaffed and overworked, leaving them struggling to keep up with minor day-to-day responsibilities, never mind ensuring that your network is as secure as possible.
- **Educate your people**. Lawyers, staff, and any other employees need to understand how data breaches happen. Many breaches are the result of simple carelessness - leaving a laptop unattended, losing their phone, or accessing your network via an unsecured public wifi network. Sensitizing your lawyers and employees to data security will go a long way toward preventing inadvertent breaches. You should also train them to recognize suspicious emails and websites.
- **Inventory and lock down your devices**. The number of phones, tablets, and laptops at your firm has likely exploded in the last few years, and it may be surprisingly difficult to keep track of them. You need to first make an inventory of all devices that have access to your network. From there, make sure that only the appropriate person has access to the device. If they aren't actually using it, have them turn it into the IT department and keep it in a secured location.

- **Require and enforce strong passwords that are changed regularly.** Constantly having to change your password is a headache, but it is essential for maintaining network security. Many data breaches are unfortunately the result of weak passwords that are rarely changed. Protecting your clients' data means requiring that network passwords meet certain standards (a combination of uppercase and lowercase, combined with numbers and special characters) and are changed regularly.

In addition to those steps, we recommend working with an outside IT/cybersecurity consulting firm. We aren't suggesting that you shouldn't trust your IT department, simply that an outside firm can provide a broader perspective. In addition, a second set of eyes may catch vulnerabilities that were missed. In fact, an outside cybersecurity firm can help you conduct a security audit designed to test your network's resilience and identify any weaknesses.

Policies and Procedures

In addition to the steps mentioned above, having written policies and procedures is a fundamental part of protecting yourself and your client's data. These policies and procedures serve three key purposes:

1. To develop and maintain routines that keep your network secure and your clients' data safe;
2. To provide clear guidance as to steps that will be taken in the event of a suspected breach or if one is detected;
3. To document your firm's efforts to guard against cybersecurity breaches and that you have an established protocol in the event that one should occur.

Of course, they can also become a little bit of a double-edged sword. Your firm's policies should be comprehensive and well-thought-out. You also need to make certain that they are up-to-date as technology is always changing and cybersecurity threats are always evolving. More importantly, your lawyers and other employees need to understand them, so conducting regular training sessions is important. Finally, you need to make sure that your policies and procedures are actually being followed - having a policy or set of procedures that no one follows not only does nothing to protect your clients but could arguably give rise to a negligence claim in addition to an ethics complaint.

An Atlanta professional liability lawyer can help your firm develop a set of policies and procedures that both protects you and your clients' data. Using the guidance provided by the ABA above, your policies should do the following:

1. Set forth all of the steps your firm takes to monitor for suspected and actual security breaches;
2. Establish a clear and concrete protocol for actions that will be taken in the event of a breach to stop the attack and prevent further loss of data;
3. Create a timeline for assessing the breach and notifying affected clients.

To meet those purposes, here are some features you should consider building into your cybersecurity policy in addition to those :

- **Easy security reporting**. Creating a separate email address or something similar can help both internal and external users easily report potential security issues they encounter. Of course, you should be regularly monitoring this channel. Your policy should establish security reporting protocols

and who will be responsible for monitoring reports.

- **Timetable for software updates**. Your policy should demonstrate a commitment to ensuring that your software is up to date. This is obviously important for antivirus software, but other software becomes vulnerable to attack when you fail to install patches and other updates. The policy should establish who is responsible for ensuring that updates occur and the period of time they will be installed once they are available.
- **Restrict access**. Give careful consideration to who needs access to what information on your network, and limit access accordingly. You also want to consider whether remote access should be more restrictive than those who are working in the office. Finally, you should immediately terminate all access for any lawyers or attorneys who leave the firm. Your policy should establish how often you will review network permissions and confirm immediate termination of access for former employees.
- **Tracking Irregularities**. You should establish a process for daily monitoring of access to your network for any irregularities. This can include unusually high data downloads or access from unusual locations.
- **Password security**. We mentioned this above, but your policy on network passwords should be reflected in your cybersecurity policy.
- **Establish vendor standards**. Your policy should also set forth any requirements that vendors, contractors, or other third-parties must meet in order to protect your network.

We recommend that you work with both your in-house IT department and an outside IT consultant in developing this policy for a few reasons. First, you want to make sure that your policy is realistic and able to be implemented at your firm. The policy is worthless if it isn't followed. Second, you want to ensure your policy reflects the current state of technology and industry standards. Third, you want to make sure your policy incorporates any "best practices" employed by other firms to guard against a data breach.

Are You Insured?

Data security is enough of an issue for lawyers that insurance carriers offer insurance coverage for cyber liability and data breach. The liability in the event of a breach can be tremendous - without insurance, a single breach can force your firm to go out of business.

If you are looking for insurance coverage, you should look for a policy that provides coverage for the following:

- Costs incurred in responding to the breach
- Costs incurred to monitor the potential consequences of the breach
- Coverage for potential extortion claims
- Coverage for any interruption of your business or loss of income
- Coverage for any and all third-party claims against your firm
- Coverage for any compensatory payments to affected clients
- Legal fees and costs incurred in defending you against any claims

You should discuss your options with your firm's insurance carrier as soon as possible. If you already have coverage, you should regularly review your policy to make sure your coverage is sufficient - your exposure could increase significantly as your practice grows.

Contact an Atlanta Professional Liability Attorney

As lawyers ourselves, we understand the importance of data security - both for ourselves and our clients. We can help you navigate the potential liability exposure and liability concerns and work closely with your IT people to ensure you have the best possible plan in place. If you'd like to discuss your needs and how we can help, call us at 678-701-9381 or contact us online to speak with an Atlanta professional liability lawyer today.