DATA PRIVACY AND CYBERSECURITY

Lawyers, Data Privacy, Cybersecurity and the Ethics Rules

By: Robert T. Egan, Esquire and Anthony M. Fassano, Esquire
Archer Law

Editor's Note:
This is the first in a series of articles by members of Archer & Greiner's **Data Privacy and Cybersecurity Practice Group** which will discuss various aspects of data privacy and cybersecurity law of interest to all lawyers, both for their own business management and to provide basic advice to their clients. This article focuses upon a lawyer's ethical obligations as applied to technologies commonly used in today's legal practice.

***

The ever-increasing dependence on technology in the legal profession brings with it an enhanced risk of cyberattack and the theft of confidential information of all types—whether belonging to clients, adversaries, or law firms themselves. Not surprisingly, traditional ethics principles have now been applied in the cyber age, imposing ethical duties upon attorneys in addition to the duties imposed by the patchwork of cyber-focused statues, regulations, and case law applicable to business of all types.

Examples of hackers stealing customer information from big companies are legion and frequently publicized in all types of media. But law firms are also common targets of cyber criminals. Lawyers are data aggregators—they collect sensitive, privileged, and personal information from a wide variety of sources, as well as create and maintain data and information on their own practices, employees and business.

Consequently, the legal profession is one industry on which the law imposes special rules and duties to protect against the unauthorized access to private information and to respond whenever that information is accessed. The ABA Model Rules of Professional Conduct ("RPC") contain several applicable provisions, and its Standing Committee on Ethics and Professional Responsibility has issued two important formal opinions on the topic.

Technological Competence and Confidentiality

Lawyers must provide competent representation[1]. Competence requires you to keep abreast of the benefits and risks of relevant technology[2]. This does not mean that you have to become an expert in computer technology. However, it does mean that, if you lack those skills, you must remedy the deficiency through education or by associating with lawyers or experts who are competent.

In addition, law firm partners and supervising lawyers are responsible for the RPC compliance of the lawyers and nonlawyers over whom they have supervisory authority[3]. This duty extends to outside vendors retained to work on discrete projects[4]. In short, you must ensure not only your own competence, but also the competence of those working under you, lawyers and nonlawyers alike.

Cyber competence is important because law firms, with their propensity to store confidential client information, also make for enticing targets. The risk that a cybercriminal will target a law firm implicates another duty: confidentiality[5]. This duty requires, among other things, that you take reasonable steps to protect your clients' confidential information.

So what happens if you are hacked and the cybercriminals steal confidential client information? Does this mean that you have run afoul of the RPC? Not necessarily. The inadvertent or unauthorized disclosure of client information does not in itself amount to a violation. Remember, cybercriminals have hacked some of the most sophisticated companies in the world. Instead, the inquiry turns on the reasonableness of your efforts to prevent the inadvertent or unauthorized disclosure[6]. Competence, either through individual knowledge or association with others, could go a long way in determining the reasonableness of your conduct.

The Obligation to Prevent Cyber Incidents

Lawyers are no doubt familiar with the term "reasonable," which permeates various legal concepts, and know that the word resists rigid definition. For cybersecurity, however, ABA offers some factors to consider when gauging the reasonableness of your efforts. These factors include the sensitivity of the information, the cost and the degree of protection of additional safeguards, and the likelihood that additional safeguards will hinder the ability to represent clients[7].

The touchstone here is reasonableness. It would behoove you to frequently revisit the ABA's factors to ensure that additional safeguards are unnecessary. While these factors defy a hard-and-fast rule, there are a couple of general guidelines. For instance, client information that has low sensitivity may be protected with standard security measures, requiring no additional safeguards[8].

On the other hand, when the subject of the communication with a client touches upon sensitive information, such as trade secrets, you should consider strong safeguards, such as encryption. When you suspect at the outset that the representation may require you to handle sensitive client information, consult with the client to make arrangements for the steps you will take to protect the data, perhaps even incorporating this information into the retention agreement[9].

Besides taking steps based upon the unique characteristics of a specific client, there are other generally applicable things you can do. The key here is to be proactive, rather than reactive. One important step is to employ or retain technology professionals with specific experience in data security to assure that you are keeping up with state-of-the-art technologies, as well as sound business practices and policies. Trusting an IT firm without that experience to keep you secure is not a good idea. Another proactive step is to develop an "incident response plan," which is a set of procedures and instructions to systematically respond to a cyberattack[10].

(Continued om Page 9)

Lawyers, Data Privacy, Cybersecurity and the Ethics Rules

(Continued from Page 8)

The Obligation to Respond to Cyber Incidents

Despite lawyers' best efforts, cyberattacks will still occur. As former FBI Director Robert Mueller once said, "there are only two types of companies: those that have been hacked and those that will be." Law firms are not exempt from this maxim.

So you get hacked, or think you've been hacked. Now what?

First, whatever you do, do not ignore it! Lawyers (or the experts with whom we should associate) should promptly take those steps necessary to stop the breach and mitigate damages. Among other things, it is essential to determine if the bad guys still have access to your computers and data. Having an incident response plan already in place could go a long way here. Also, notify your carrier if you have cyber insurance coverage, whether as part of a general liability policy or a cyber-specific policy (which you should obtain through a broker experienced in cyber insurance). After you stop the breach, make reasonable efforts to restore computer operations to allow you to meet clients' need[11].

After these initial steps, conduct a post-breach investigation and take steps to determine what occurred (e.g., what files were accessed, what was lost, etc.). This step is essential for communicating accurate information about the breach to clients. It may also provide information about vulnerabilities and allow for greater protection in the future[12].

Next, inform your current clients affected by the breach. This communication must include, at a minimum, the fact of the breach, the known extent to which the client's information was affected, and your efforts in determining the extent of the breach. In addition, tell the clients about your plan to respond to the breach, including efforts to recover the information lost and increase future security. Finally, keep clients apprised of developments in the post-incident investigation[13].

The ABA does not recognize the same duties for former clients. However, the ABA does recommend that you reach agreements with clients before the termination of the representation regarding how you will handle the client's electronic information after the representation ends[14].

Finally, statutes, regulations, and case law other than the ethics rules and opinions also impose obligations to prevent and report cyberattacks on organizations in general. These laws may apply to lawyers depending upon the circumstances, including the nature of the information accessed or stolen. We will tackle these issues in the articles that will appear in this space in the coming months.

For more information, or if you have any questions regarding cybersecurity matters in general, please contact ***Archer's Privacy and Cybersecurity Group*** members ***Robert T. Egan*** at ***856-354-3079*** or ***regan@archerlaw.com*** or ***Anthony M. Fassano*** at ***856-616-2618*** or ***afassano@archerlaw.com***

DISCLAIMER: This client advisory is for general information purposes only. It does not constitute legal or tax advice, and may not be used and relied upon as a substitute for legal or tax advice regarding a specific issue or problem. Advice should be obtained from a qualified attorney or tax practitioner licensed to practice in the jurisdiction where that advice is sought.

[1] RPC 1.1.
[2] RPC 1.1, Comment 8.
[3] RPC 5.1.
[4] RPC 5.3, Comment 3.
[5] RPC 1.6.
[6] RPC 1.6, Comment 18.
[7] ABA Formal Opinion 477R: Securing Communications of Protected Client Information.
[8] Id.
[9] Id.
[10] ABA Formal Opinion 483: Lawyers' Obligations After an Electronic Data Breach or Attack.
[11] Id.
[12] Id.
[13] Id.
[14] Id.

YOUNG LAWYERS COMMITTEE 5TH ANNUAL CHILI COOK-OFF RAISES RECORD $4,000 FOR VETERAN'S HAVEN!

The Young Lawyers Committee hosted the 5th annual Chili Cook-Off for a Cause on March 2, 2019 at American Legion Post 371. 60 people attended this fantastic event, and a record 13 different chilis and various cornbread, side items and desserts were entered into the competition. In the end, Braheme Days won first place for both chili and cornbread, with Abe Tran taking home the bragging rights for his first place dessert. Special thanks to our terrific sponsors Law Office of Vincent Ciecka; DeMichele & DeMichele; McDowell Law; Locks Law Firm; Stradley Ronan and Brian Herman & Tom Hagner. The event was a huge success!