GPSOLO

Cyber Insurance and Information Security

Kathleen Balthrop Havener

In 1976, students at the University of Alabama who participated in the Law School's second-year moot court competition faced a hypothetical case involving stand-alone mechanical devices that used optical scanning equipment and a telephone data connection to dispense a fixed amount of cash when a user inserted a specially coded card. Before I became (vicariously) familiar with that one moot court problem, I had never heard of an automated teller machine. It was still a dozen years or more before the term "ATM" was in widespread use. By 2015, though, it was estimated that there were at least 3 million ATMs operating worldwide. And to think that today I can safely make deposits into my bank account without changing from my PJs!

The technological changes during the years I have been exposed to the legal profession are almost impossible to comprehend. We have progressed from stenographers, yellow paper pads, and IBM Selectrics to voice-recognition software, incalculable amounts of data stored in the cloud, and keyboards too small for our clumsy thumbs. Document productions have changed from countless heavy boxes of dog-eared pages in dusty warehouses to images and native formats produced via data connections almost none of us understands.

Given our reliance on communication and storage of information via technology, is it any wonder that "black hats" who know more than we do spend their time and energy trying to figure out ways to misdirect that information for profit?

It is a wonder that, regardless of how much time and energy (not to mention treasure) we spend protecting our clients' interests, so few of us spend similar time, energy, and treasure protecting our clients' confidential information. In 2016, the American Bar Association's Legal Technology Survey results revealed that only half of law firms with 500 lawyers or more had plans in place to deal with security breaches, and only 17.1 percent of all firms had such plans. This is so even though a client's

sensitive information can be intercepted as easily as one can mislay a cell phone or leave a laptop in a taxi.

In December 2016 the U.S. Attorney in Manhattan charged three Chinese citizens with trading in information obtained by hacking into a number of law firms advising clients involved in mergers and acquisitions. According to the *New York Times,* the hackers targeted at least seven firms and succeeded in penetrating the information systems of at least two of them. They stole e-mails of partners who were working on particular mergers. The hackers then used information about upcoming mergers to trade in securities, profiting at least $3 million in the process. The information the hackers obtained included which enterprises were looking at mergers or acquisitions, the timing of deals, and even pricing details.

Preet Bharara, then the U.S. Attorney for New York's Southern District, said "this case of cyber meets securities fraud should serve as a wake-up call for law firms around the world: you are and will be targets of cyber hacking, because you have information valuable to would-be criminals" (tinyurl.com/mpxdcmh).

Lest you think your small practice is immune, ask yourself whether you have information stored in your law firm's computers or information systems that would be valuable, not necessarily to potential criminals, but to anyone. You might believe that opposing counsel is above hacking into your system and combing through your computer files. But is the opposing party? How about that nutty ex-spouse in a bitter divorce or custody case? Would a competitor use underhanded cyber tactics to try to steal your client's innovations? Corporate espionage has become commonplace. Will a porous firewall prick the conscience of a thief more than a shoddy lock or a paper file left unattended?

The Rise of Cyber Insurance

Providers of professional insurance products predict that insurance coverage for information security breaches, typically referred to as "cyber insurance," will eventually become a basic element of every law firm's insurance coverage, as ubiquitous as property insurance for brick-and-mortar businesses or health insurance for individuals. Moreover, sophisticated clients have begun to demand that their legal representatives insure at least as much as the clients themselves that their most confidential information is protected and secure.

It is no surprise that law firms that obtain and maintain cyber insurance are also the most likely to have the most well-honed cybersecurity policies in place. Just as having a security alarm system

installed in your home lowers your homeowner's insurance premium and an automated docketing system lowers your malpractice premium, the very process of acquiring cyber insurance increases your preparedness and decreases the likelihood of significant loss owing to security breach. Because your firm goes through an underwriting process before it is able to purchase coverage, you will have the opportunity to learn about particular security practices that render your firm's and your clients' confidential information safer than before you sought coverage in the first place.

If you don't even know where to look for cyber insurance, it's always a good idea to contact your state bar. It's very likely the staff there (probably in "member services") can steer you to several sources. As recently as late February 2017, the American Bar Association (ABA) expanded its insurance program to offer cybersecurity coverage.

Preparing for Cyber Insurance

Let's talk basics. I mean really basics. Exactly what are we talking about insuring? Before we go there, what does your firm do to protect information on paper? Are your file cabinets locked? Are shredders easily accessible? Are document disposal policies in place (and adhered to)? Have you a document retention policy? What about a clean desk policy (at least for any room to which outsiders have access)? Wells Fargo's Insurance Division reported in an August 2016 white paper that 22 percent of its survey respondents reported information loss from a "paper breach"—most commonly because of improper disposal or loss by an employee.

The same ideas translate to the computer world. Even a ten-step verification process to allow employees to transmit data wirelessly is useless if an employee is permitted to store sensitive documents to her computer desktop on an unprotected computer.

When you first seek cyber insurance, the first step of course is to fill out an application. The application will ask you what protections already are in place. Is there a secondary backup computer system? Do you have a business continuity plan? A disaster recovery plan? More critically, does your firm have an incident response plan (IRP) for network intrusions and virus incidents?

One professional insurance broker told me that most of the lawyers who telephone with the idea of purchasing cyber insurance have little to no idea even of what questions they ought to be asking, much less what coverage they need. Fortunately, there are companies that can help you explore your systems' vulnerabilities and educate yourself about what you need. Some underwriters require a "tabletop exercise" that tests and/or develops an individualized IRP. Here's an example:

You are a senior attorney in your six-lawyer firm, neither the managing partner nor a newbie. Your mailbox dings that you have a new message. You don't recognize the sender so you check the e-mail address. It looks legitimate. Perhaps a colleague has a new assistant. You even think you recognize the subject matter. It isn't related to your practice. You believe it's the results of a survey your committee helped prepare for the local bar association. You open the attachment to check out the data.

Except it isn't data and the e-mail address was an imposter's. The attachment is malware. By the time you realize what you've done, it's infected your computer and every other computer on the network. Now what?

What comes next is your IRP. What does the IRP specify? Likely, you shut down the network immediately. You run virus/malware recognition and removal software on every computer and mobile device in the firm. Once you've located where the virus originated—making sure that all the others have been cleaned of viruses—the network goes back online and the single infected hard drive is wiped.

(Yes, it might be a huge headache. Your partner in a three-day trial in Nebraska may be seriously inconvenienced. But it's better than corrupting every computer file in the firm.)

In the future, one hopes, such malware will be detected before an e-mail is opened and "quarantined." Some websites are blocked altogether—they can't be accessed except on particular computers used specifically for that purpose—because the websites are known to be sources of viruses or malware.

There are companies whose business it is to help you test your systems and design an IRP. Such a plan is more specific and more highly particularized than crisis management policies. Typically, IRPs clearly specify the roles of individuals and the steps that must be taken when a breach occurs. Before finalizing a plan, the company you engage should perform "penetration testing" to learn where the firm's vulnerabilities are and plug any holes.

And exactly what are you paying for when you insure against cyber threats? Like any insurance question, the answer is always, "it depends." What's the information you're protecting, and what do you have to do if it's stolen, corrupted, or lost? Do you want your insurance to cover the costs of notification of clients that their information may have been compromised? Will the insurer pay for defense costs if the firm is sued? Will there be business interruption coverage? There may be privacy issues, regulatory requirements, and media involvement.

Where to Start

There can be no question that law firms are behind the curve on the cybersecurity issues. It's not hard to figure out why. Security costs. The latest software is expensive. Protection against viruses and malware costs money. And although your clients' information is what is at risk, you can't pass the cost of securing their information on to them.

The glaring truth is that few firms—small firms and sole practitioners in particular—are prepared for a major information breach. The ABA is trying to fill the void. It has established a Cybersecurity Legal Task Force, and the second edition of the *ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals* is expected to be published in 2017. It's a primer that will at least familiarize you with the terminology and the basic information to help you decide what you need.

You say you don't know where to start? Call your malpractice insurance broker. The broker will guide you through engaging a cybersecurity consulting firm if you need one. If not, the process of obtaining cyber insurance will sufficiently educate you about what changes you need to make—individually or for your firm—to comply with client expectations and ethical requirements.

Before you start spending sleepless nights obsessing about the safety of your law firm's and your clients' information, remember the words my very wise mother used to tell me: "Worrying is like trying to solve a geometry problem by chewing bubble gum." Fretting about your law practice's cybersecurity is a similarly useless enterprise. Still, you can at least call your broker and get the process underway. In the process of obtaining coverage, you'll gain more than just financial protection against loss. You'll acquire an understanding of what you really need to do to protect against cyber risk and why you need to do it. Lawyers deal in reputation management. Pay attention to yours and guard it from attack.

Educate yourself and your employees. That's by far the most important investment.

Authors