What a difference four years makes! Since the first edition of this book was published in 2012, there has been a veritable revolution in information security. Four years ago, many lawyers were largely ignoring information security, content in general to delegate the responsibility for it to someone else.

No more. These days, lawyers are really running scared. So many law firms have been breached. And as the saying goes, there are two kinds of law firms; those who have been breached and those who will be breached.

Today, when we lecture on encryption, we have standing-room-only audiences. The people who come to our live sessions radiate a hunger for cybersecurity knowledge. They are genuinely scared—and perhaps more so because of the new versions of the ABA Rules of Professional Conduct 1.1 (Competence) and 1.6 (Confidentiality of Information), which together require competent and reasonable measures to safeguard information relating to clients. As we go to press, twenty states have adopted the changes to those rules—and it is clear that more states will be following suit soon.

This book, like its predecessor, sets out to make information security a little more approachable. There needs to be some technical explanations of course, but we’ve tried to keep the technical stuff to a minimum so that the average attorney can genuinely understand the security demons that are out there and how to defend against them. Forewarned really is forearmed.
Much of it is not a DIY sort of project, especially if you’ve suffered a security breach. We make no attempt in this book to document the myriad steps that a professional information security expert would take. Our objective is to teach the data security basics in language that can be readily understood by lawyers. If you’re in over your head, you’ll hear us advise you again and again to seek professional help. Even among those who call themselves experts, there is often a shocking knowledge shortfall or a failure to keep up with current developments, which happen with dizzying speed!

One of the greatest difficulties of information security is that it is a moving target and that target has been moving faster and faster in the last four years. The landscape of threats and defenses to those threats changes so quickly that last year’s (and sometimes even yesterday’s) knowledge is woefully inadequate to combat today’s perils. “Eternal vigilance” is absolutely required for those of us who deal with data security issues.

Still, there are guiding principles that remain largely the same. We have tried to break information security down into digestible segments, knowing that some attorneys will pick up this book with concrete questions about specific security areas. Common questions we hear include:

1. How do I secure my computers and networks?
2. What constitutes a strong password today?
3. Are passwords dead?
4. What is multifactor authentication?
5. How do I secure my smartphone?
6. Do I need to encrypt all my devices?
7. Can I safely use my laptop at Starbucks?
8. And the big kahuna is the question about what is ethically required—and our answer to that has evolved.

We are now at the point where encryption should be deployed by all attorneys, where appropriate—and it is so cheap and simple to use these days—even to encrypt e-mail—that there is no longer any reason not to do so.

If your interests in cybersecurity are narrow, you should be able to find what you’re looking for by scanning the Table of Contents. We would urge lawyers, however, to take a broad interest in the security of data because they have, unlike the general public, professional and ethical requirements to safeguard client data.
Although lawyers are all aware of ABA Model Rule 1.6 (and we have an entire chapter on an attorney’s duties to safeguard confidential data), the challenge is how to keep client data secure in the digital era. It isn’t easy and continues to become more difficult. The paper world was much simpler to lock down. The earlier days of information security, while challenging, were also simpler than today. It is much more difficult now that we have moved from individual computers and isolated networks, with limited connectivity, to the Internet, almost universal connectivity, and widespread mobility. The term du jour is now “cybersecurity”—focusing on cyberspace and connectivity. But cybersecurity is actually a subset of information security because individual computers, servers, and mobile devices need to be protected from threats like loss, theft, and unauthorized physical access—distinct from cyberspace. Information security can be expensive—and it takes time and effort to understand it—and you will never finish learning because threats, defenses and technology morph constantly.

Are lawyers doing enough to safeguard law firm and client information? Our opinion is that many are not. Here are a few reasons we hold that opinion.

♦ The FBI reported at a legal technology conference in 2013 that they are seeing hundreds of law firms being increasingly targeted by hackers.

♦ Mandiant, now part of InfoSec giant FireEye, reported that 7% of the breaches it investigated in 2014 involved law firms.

♦ Another report noted that 80% of the one hundred largest law firms, by revenue, had been hacked between 2011 and 2015.

♦ At a meeting of large firm information security experts from Washington, D.C., most admitted that they had been breached—and that they were aware from their colleagues that others had been breached as well.

♦ Even with the dismal record of reporting law firm data breaches, we still learn of them in the press and informally—and we will detail some of them for you.

While data breaches can happen despite reasonable (or even stronger) security, the frequency of law firm data breaches and reports on how some of them have occurred suggest that many attorneys have not been employing reasonable safeguards. Why do many otherwise competent lawyers fail so miserably in protecting firm and client data? Here are some of the reasons.
Lack of knowledge—they simply need education—and many of them don’t know they need education.

The “it can’t happen here” mentality is flatly wrong. Since the FBI issued an advisory in 2009 warning that law firms were specifically being targeted by identity thieves and by those performing business espionage, it has continued to meet with large firms to preach the gospel of information security. We were, in the earlier day, worried about cybercriminals, China, and other state-sponsored hackers, which continue to be major threats. Thanks to Edward Snowden, we now know that we also need to worry about surveillance by our own government.

According to press reports, lawyers and law firms are considered “soft targets”; they have high-value information that’s well organized and frequently have weak security—although we are happy to report that, at least at large firms, cybersecurity is now a very high priority.

Though there are many low cost/free measures that solo and small-firm lawyers can take to protect sensitive data, true information security, including hardware, software, training, etc. is expensive. Protecting the security of client data can present a big burden for solos and small law firms. This does not take away a lawyer’s ethical duty, however, and it is one reason the authors lecture so often on computer security. Once a lawyer sees the most common vulnerabilities, he or she can take remedial steps—or engage an IT (information technology) consultant to do those things that are beyond the lawyer’s skill.

The need for vigilance never stops. You cannot secure your data once and think you’re finished; the rules of information security change on close to a daily basis. Certainly, someone in the firm needs to keep up with changes on a regular basis or the firm needs to engage a security consultant to do periodic reviews. While the necessary frequency of security assessments depends on the size of the firm, the sensitivity of the information, and identified threats, it is our judgment that mandatory assessments should be conducted at least annually. And clients are beginning to demand self-audits and third-party audits of law firm security. Sensei has never seen a client who passed such an audit on the first go-round. In fact, they don’t even understand the audit questions, which doesn’t bode well for the results.

In the paper world, keeping client data confidential was easy and cheap. In the digital era, abiding by this particular ethical rule is often hard and expensive, but it must be done. We hope this book takes some of the
“hard” away and also helps lawyers understand how many inexpensive steps exist to protect data without breaking the bank.

Often, this subject seems so dense and unapproachable that lawyers have suffered the “ostrich effect” and simply bury their heads in the sand. Fortunately, as clients have woken up to the potential vulnerabilities of law firms, they are demanding much, much more in the way of security—it is clear that clients are leaving firms that don’t meet their security expectations. Hence, the fairly sudden desire to get secure. In the AmLaw 200, firms are now reported to be spending an average of 1.9% of gross revenues on cybersecurity—and that can amount to as much as $7 million a year. That is an extraordinary change, to say the least.

In the American Bar Association’s 2015 Legal Technology Survey Report, it was clear that data breaches continue to increase, especially at larger firms, which no doubt hold the most valuable information, although smaller firms handle valuable data too, such as those practicing family law. We’ll go into more details from that survey later in this book.

We certainly are seeing an increasing focus on information security in large firms, but the trend as you go down the food chain is still too often to “hope for the best” after taking a minimum of security precautions. Smaller law firms are not used to budgeting for information security, and yet this is clearly mandated in a world where technology rules us all. The crown jewels of law firms are their electronic files, and yet many law firms guard them sloppily.

And if you think your insurance policy will protect you, think again. Be sure to read the chapter on cyberinsurance. We can just about guarantee that what you read in that chapter will make you go through your current policy with a fine-tooth comb and consider the need for additional coverage.

For years, we’ve been warning lawyers that it’s not a question of whether law firms will become victims of successful hacking attacks; rather, it’s a matter of when. We pointed to incidents of dishonest insiders and lost or stolen laptops and portable media. We’ve now reached the when—there have been numerous disclosed incidents of successful hacking attacks on law firms by cybercriminals and foreign governments and interests, and there is now a threat of NSA surveillance of law firms. The truth is that everyone is watching—governments (including our own), hackers, cybercriminals, competing businesses, etc.

We have even heard of two cases in 2015 where law firms allegedly hired hackers in order to glean information about their opponents in a case—
more on those later—and any like-minded lawyers need to read our ethics chapter!

We have included in this book security approaches, products, and solutions about which we have sufficient experience or information to include them. There are additional security approaches, products, and solutions that we could not cover in a book of this length. In addition, there will certainly be changes in technology, threats, and available safeguards, some rapidly evolving. Because of future developments and additional options, it is best to make sure that you have current information when selecting and implementing safeguards. Ask someone who stays current on information security or check reliable online resources. Chapter 27, Additional Information Resources, includes a comprehensive list of sources, starting with our Short List of Favorite Information Sources.

We have set out in this book to provide practical advice in a condensed format. We hope that sharing some of the InfoSec “war stories” by way of examples will serve to make a business case for genuinely focusing on information security on a regular basis and, depending on the size of your firm, the sensitivity of the information and your area of practice, making sure that sufficient funds, time, and attention are allocated to protecting your firm’s data.