

# A Cybersecurity Handbook for All Attorneys and Law Firms

BY SHAWN E. TUMA

Cybersecurity is one of the most important issues of our time and one that most certainly will impact all attorneys and law firms across the entire spectrum of practices. Despite the importance of this issue for the legal profession, most of the information written about cybersecurity is not very usable by practicing attorneys and, in many cases, makes it seem as though being cyber secure is only important to the largest of law firms—and out of reach to all others.

Recognizing this need, in the second edition of their book, *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals* (ABA Publishing, 2017), editors Jill D. Rhodes and Robert S. Litt assembled an all-star team of 26 well-respected practitioners who share their expertise with the readers. This book, written by practicing lawyers for practicing lawyers, is 464 pages full of substantive content that goes from high-level, easy-to-read top 10 lists that even the most technophobe lawyer can use all the way down into the weeds of deep technology, cybersecurity, and legal analysis that even the most advanced readers will find valuable. The focus on practicality is what makes it so useful.

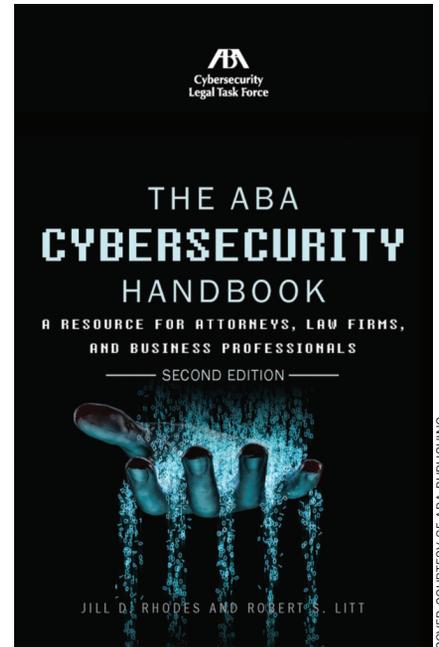
The *Handbook* provides helpful guidance for attorneys who practice in every type of setting across all practice areas. Whether it is a solo attorney doing probate work in a rural county looking for a few simple tips, the attorney practicing in the international firm counseling clients on substantive cybersecurity and data privacy issues, or in-house counsel, government lawyers, and public interest lawyers, they will all find the *Handbook* helpful.

The authors avoid much of the hysteria and fearmongering we often hear with cybersecurity. Instead, they provide clear examples of the risks and practical

**This book, written by practicing lawyers for practicing lawyers, is 464 pages full of substantive content that goes from high-level, easy-to-read top 10 lists that even the most technophobe lawyer can use all the way down into the weeds of deep technology, cybersecurity, and legal analysis that even the most advanced readers will find valuable.**

solutions to the problems. The book addresses how cybersecurity risks apply to attorneys and law firms in particular and why legal and ethical obligations require lawyers to protect against those risks, and provides practical solutions for how attorneys and law firms at every level can help protect against those risks. This is reflected in the organization of the book, which is broken down into four primary sections: (1) cybersecurity background and risks and common forms of attack, especially against attorneys and law firms; (2) lawyers' legal and ethical obligations for protecting their networks and client data; (3) application to different legal practice settings from large to small law firms, in-house counsel, government lawyers, and public interest attorneys; and (4) guidance on incident response and cyber insurance issues.

Most larger and more sophisticated firms are addressing cybersecurity because their clients are demanding that they do so or else they will not send them business. The attorneys that frequently need the



COVER COURTESY OF ABA PUBLISHING

most help are the solo and small-firm practitioners that do not have the information technology and cybersecurity teams in place. This book provides excellent straightforward advice to them in Chapter 9, "Cybersecurity for the Little Guys." The introductory paragraph sums up my experiences in this area quite nicely:

I can hear some lawyers saying it now: "I'm just a solo. I don't need a complicated computer security system. Nobody is interested in me. Besides, I don't have an IT department to handle it or a big budget to spend on computer security. This is just for the big firms."

The chapter goes on to explain why this thinking is not only incorrect on several levels, but provides 12 specific steps solos and small firms can take, with explanations and a table for checking off completions, for effectively improving their cybersecurity. **TBJ**

For more information about cybersecurity from the American Bar Association, go to [ambar.org/cyber](http://ambar.org/cyber).



## SHAWN E. TUMA

is an attorney widely recognized in data privacy and cybersecurity law, areas in which he has practiced for over two decades. He is co-chair of the Data Privacy and Cybersecurity

Practice Group at Spencer Fane and works primarily in the firm's Collin County and Dallas offices.