CHAPTER 1

# The Need for Cybersecurity

This book was written to help you take control of your cybersecurity. Every day in the news, we read about cybercrime—a multi-billion-dollar-a-year criminal industry whose actors have little fear of law enforcement. Incidents of cybercrime and cybercrime-related identity theft continue to grow exponentially. As a result, governments, regulators, and professional bodies increasingly require that lawyers and other professionals take reasonable cybersecurity measures. Beyond protecting our workplaces from cybertheft or intrusion, we also need to protect ourselves and our families from these threats.

Why is there so much concern about cybercrime and cybersecurity? Here is the basic problem: When we use the Internet, we drastically increase the odds that private and confidential information in our possession will be stolen. Not long ago, it was nearly impossible for criminals to steal all of your confidential documents, correspondence, photos, and other personal or professional information. They would have had to pick your pocket, burglarize both your home and office, and manage to carry it all away without being caught. Today, vast quantities of documents, data, photos, and personal and professional information are on our phones, laptops, and in the cloud. A cybercriminal can steal it all through the Internet, without you even knowing that anything has happened. The information that was once contained in hundreds of boxes of paper documents—and required a moving van to take—now exists in bits and bytes, and can be stolen with the press of a button, remotely, from thousands of miles away.

This type of data is valuable to criminals. They can use personal information to steal in any number of ways, to include tricking banks and credit card companies into giving them money or credit in the victim's name. Personal data has become a commodity, sold on the black market for its intrinsic value. Criminals even use encryption to "lock up" data, and then extort the data's owner for ransom in exchange for access—so-called ransomware. Imagine if all of your personal and client files were suddenly unavailable to you. And while greed is the main reason cyberthieves want your data, there are other reasons, too, such as harassment, stalking, and corporate espionage.

The Internet makes cybercrime possible. It is the information "superhighway," and our devices are continuously connected and ready to send and receive information from friends, family, employers, colleagues, clients, financial institutions, retailers, advertisers, and many others. Data is being exchanged constantly. This perpetual connection means our electronic door to the Internet is visible to the world, thereby exposing us to criminals. These criminals, like house burglars, are always trying doorknobs, hoping for an unlocked door. If that fails, they will knock on doors to try to talk their way in, see if they can pick the locks, or even kick doors in.

## WHY THIS BOOK?

Most of us have neither considered, nor know how "cybersecure" we are. If you are not an information technology (IT) professional, the idea of delving into the technical details of secure computing can create apprehension and confusion. Some people think that if their e-mail system works, and if their documents are accessible, then why bother making any security improvements to their system, which might create complications or cost time and money. Some would prefer not to know the cybercrime risks they are facing, or just haven't thought about it. Cybersecurity is more, though; it is also about protecting data from risks other than cybercrime, such as unanticipated IT issues, hard drive crashes, house fires, and other incidents. Beyond security, this book will also help you use your computers and data more efficiently.

No matter your level of comfort or experience with computers, this book will help you recognize when your electronic "doors" are open to cybercriminals, and help you fully appreciate why you need to take certain security steps. Since cybercriminals are always attacking, trying to steal your data or make your data unusable, this book will help you understand these risks so you can decide where to set your "cybersecurity dial" in your home and office. How much risk feels comfortable? How sensitive or confidential is your data? Are you safeguarding someone else's data and confidential information? What do you risk, professionally and personally, were your data ever stolen or compromised? If you set the dial too low, you may be overly exposed to threats, but if you set the dial too high, you may become frustrated with the inconveniences of the security measures themselves. Appendices 1 through 4 offer some assessments and materials to start your thought process about your cybersecurity posture and awareness. Appendices 1 and 2 have short quizzes you can take to assess your current security, awareness, and threats, and see how your home and work cybersecurity are related. Appendix 3 discusses the concept of the cybersecurity dial, where it is set now, and where you want it to be. Appendix 4 covers some common cybersecurity myths.

Cybersecurity is not one-size-fits-all, but needs to be what works for you. It's how you decide to evaluate and manage your risks. With this book, you can gradually increase your security posture as you learn, by making incremental changes and learning to live with them. For the price of this book, you will learn how to improve your cybersecurity by yourself, without paying anyone else to do it for you, as this book does not recommend any costly services or products. The time you invest now can save you from an expensive disaster later and could make your computing experience much more efficient. By first fixing the cybersecurity of your home and personal devices, you will then be in a position to translate that knowledge and experience to your workplace.

I wrote this book for other lawyers because we all have personal and work-related information on numerous devices and in various locations, and we all should be aware of the risks of loss or theft of that information. I have had the opportunity to learn about cybercrime, cybersecurity, law, and the basic mistakes most people make that puts their information at risk.

You should not wait for the law and other standards to evolve, as they will always lag behind the pace of technology advancements. The basic principles and methods to secure yourself are available now, and you can learn and apply them yourself. Technology will continue to change rapidly, but if you understand the basic principles, you will be able to make sound, ongoing choices to protect yourself.

You need not become a technology expert; however, you should learn about the serious threats you face, the potential consequences, and the steps you can take to mitigate these risks. Technology-related threats and appropriate countermeasures are similar to things you already do in your "brick and mortar" physical life. This book will teach you to secure your computer just as you learned to lock your house's doors and windows, put on your seatbelt while driving, check your car's oil level and tire pressure, and stop at a red light. Yes, computers can be complex, frustrating, and confusing, but everyone can learn how to do this.

## WHAT YOU SHOULD DO RIGHT NOW

I hope you will read all of this book—doing so will improve your security to the degree that you choose, even if that is just a little bit. If you read this book in its entirety, you will understand the concepts and risks, improve your own protection, and be able to thoughtfully discuss cybersecurity issues with your clients, friends, and family members. Cybersecurity will no longer be a daunting issue for you.

I know that many things compete for your time, and it might take a while to get through this book in its entirety. There are some important concepts

you should remember, and steps you should implement as soon as possible. If you remember nothing else, *remember* these key concepts:

1. Your data has value to cybercriminals—they will try to steal it, sell it, and use it.
2. Your data has value to you. Losing access to your data would be devastating. Cybercriminals may lock you out of your data in order to extort payment for its return, or to use the data themselves.
3. You can make small changes that will greatly increase your security, without interfering with your regular computer usage.

If you do nothing else, *implement* these simple steps to improve your security:

1. Put a password or passphrase on all of your computing devices (smartphones, tablets, laptops, and desktops). Make it easy for you to remember but difficult for a stranger to guess.
2. For your e-mail and cloud accounts, have a more complex password or passphrase, but recognize that a password alone is not always enough. Add a second measure to gain access, such as a one-time code that the provider sends to your cell phone. This is called "two-factor authentication" or "two-step login."
3. Run anti-malware software on your laptop and desktop. You can find free software from reputable companies that works well for this purpose.
4. Disconnect from the Internet (or turn off your devices) when they are not needed.

## HOW THIS BOOK IS ORGANIZED

The first half of this book provides a basic understanding of the threats you face from criminals, examines the interests of advertisers in acquiring your personal data, and offers a foundational understanding of information security principles and how computers and networks work. When a threat is discussed, there is a quick tip on how to protect yourself from it; but, mostly, this part provides a basic understanding so that when you read the second part of the book, you will be able to make informed decisions.

The second half of this book starts with Chapter 7, and helps you protect yourself in a systematic, incremental manner, as you gradually learn about and improve your security posture and knowledge of the systems you use. This will help you decide where to set your "security dial," and guide you as you safeguard your computing devices. Then you will effectively protect the data that you maintain on your devices, in the cloud, and in your online

accounts, as well as the information that you provide to others. The following chapter will secure your home network, and hone the way you use the Internet and the "Internet of Things." Then it's time to apply what you've learned to protect your family.

Next, you'll learn how to travel securely with technology; then we will look at how all of these principles translate to your work setting. In Chapter 14, you'll learn about the professional responsibilities you have as a lawyer with respect to your own cybersecurity, and you'll get a quick primer on the law as it applies to you and your clients. The last chapter is about troubleshooting for cybersecurity and other IT issues. The appendices have more detailed materials to help with your cybersecurity and IT awareness and implementation, additional resources, and helpful fill-in-the-blank forms. These forms can also be downloaded at CybersecurityHomeAndOffice.com, a website that also contains materials that parallel the book, such as photos of computer components that could not be included here.

## YOU *CAN* IMPROVE YOUR OWN CYBERSECURITY

Whoever you are, and whatever your background, you can improve your home and office security by taking simple steps to safeguard your computers and data. You don't have to become a computer expert to protect yourself, and, with the help of this book, can start building some good cybersecurity habits that will translate directly to the workplace. Once they become habits, the steps will be nearly effortless and keep you safer. This book is not meant to scare or shame you, and it will not advise you to take every single precaution to guard against every single threat. Rather, it will empower you to learn and to understand, so you can make your own choices to protect yourself better.