Preface

Daniel Garrie

In our society, law firms have long held the position of being problem solvers. They untangle the mess of business, and create rules for society. Since their inception, law firms have devoted significant resources to ensuring the best representation of their clients. But now there are new threats that law firms face beyond the practice of law, namely data breaches and cyberattacks, and they must begin to devote sufficient resources to ensuring the security of their clients’ data. If a firm is breached, its client files may inadvertently end up on the darknet, in the hands of investigative journalists, or with other nefarious entities.

Consider the following hypothetical: A small law firm did not have proper access controls for different employees, so any employee could access the highly sensitive data of all the firm’s clients. One day, a new associate decides to poke around the firm’s files, and finds that the firm has been assisting a local bank in evicting his grandfather from his home. This attorney rashly collects and leaks all of the firm’s files, leaving the firm scrambling to figure out what happened, how these documents were leaked, and how to stop and control the subsequent reputational fallout to both the law firm and its clients.

This example is not meant to scare lawyers out of the practice of law, but rather to serve as an explanation of the seriousness of a data breach in the law firm context, and a reminder of why investing in information security is prudent. Law firms, both big and small, need to become cognizant of the risks associated with a data breach, and determine how to protect and secure their clients’ confidential data.

Law firms can mitigate the risk of a data breach through a variety of means, including investing in cybersecurity tools, hiring internal and external resources to augment the firm’s current information security practices, and—arguably most importantly—changing the firm’s culture to be more security conscious. Although no one-size-fits-all solution exists for dealing with cyber threats, with proper focus and resources, a firm can consider its unique factors and develop an information security posture that addresses its most compelling concerns.

While preventing a breach should be a paramount concern for any law firm, it is similarly important to prepare for what could happen in the event that a breach occurs. There are options, such as cyber insurance, to help mitigate the direct costs
of a breach, but law firms must also look to other options to resolve these issues expeditiously. As the costs associated with litigating data breach claims continues to climb, it will become increasingly apparent that law firms must begin looking toward other dispute resolution mechanisms, such as arbitration, to mitigate and control costs. This book hopes to give firms information about the tools they need to defend themselves; however, firms must also take steps to create processes to mitigate and control the risk of and fallout from a data breach.