bookreview

The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals

Jill D. Rhodes and Vincent I. Polley

"There are two types of firms: those that know they've been (cyber) attacked and those that don't," says Jill Rhodes, co-author along with Vincent Polley of the *The ABA Cybersecurity Handbook*. The book is an initiative of the ABA Cybersecurity Legal Task Force that was created in 2012 to bring together the legal community and private sector to help secure law firm computer systems.

As described throughout this issue of *LawPRO Magazine*, law firms (as well as government and in-house lawyers) are tempting targets because of the wealth of confidential information they have about their clients, such as strategic business data, proposed mergers and acquisitions, intellectual property and information obtained through e-discovery in the course of litigation. And it isn't just hackers that can cause these breaches: it could be disgruntled or duped employees, lost mobile phones with lax passwords, or accidental damage (e.g. a flood) to computer hardware resulting in a malfunction of security systems.

This book was written as a resource for lawyers in all practice settings to help them develop a cybersecurity strategy. There is no single solution for every firm, and developing measures to increase security and respond to breaches requires balancing legal requirements, firm resources, staff training, investments in technology and client needs.

The authors first look at why firms are vulnerable and what steps they should be taking to increase their cybersecurity. The underlying problem is that lawyers are experts on law, not technology, and often don't have the kind of security arrangements big businesses or governments do. Data that was created in a secure environment can become exposed when it moves into the hands of a law firm with inferior security systems. Firms are under pressure to find efficiencies such as outsourcing, cloud storage and mobile devices, and each of these ways of dispersing client data adds another potential breach point. Lawyers and staff may also resist new security arrangements and the inconveniences these can bring.

At the same time, the authors point out that lawyers fundamentally understand the importance of client confidentiality, and that's a good starting point to make them embrace the importance of improved cybersecurity. Also, clients will increasingly press firms to have security systems as strong as their own.

The book describes how firms should do a risk assessment and develop plans to not only prevent security breaches, but also deal with them when they happen (and firms should make the assumption that breaches *will* happen). This assessment would cover all of a firm's data usage policies and the ways in which staff use and access confidential data. How to have a conversation with clients about data security (in terms of potential added costs and what to do in the event of a breach) would also be considered.

The next section of the book is an in-depth look at the legal and ethical obligations lawyers have to protect clients' data. As the book was written for a U.S. audience, the rules and laws described apply to American lawyers. However the basic principles would apply to Ontario lawyers, who will want to consider the Law Society *Rules of Professional Conduct* and bylaws as well.

The remainder of the book looks at how firms of various sizes can implement cybersecurity strategies. Small firms will have the flexibility to adopt new technologies and practices quickly, but may struggle with the costs, while large firms would have the opposite challenge. The authors also address how government and in-house lawyers can improve their levels of security.

For many firms, issues of cyber and data security have crept up on them in recent years, but recent high profile breaches of client information have added a sense of urgency. This book is a good resource for firms wanting to start a discussion with staff, clients and technical support providers about their own state of preparedness for a cyber attack or data breach. ■

Tim Lemieux is practicePRO coordinator at LawPRO.

About the practicePRO Lending Library

The practicePRO Lending Library has more than 100 books on a wide variety of law practice management topics. Ontario lawyers can borrow books in person or via e-mail. A full catalogue of books is available online (practicepro.ca/library). Books can be borrowed for three weeks. LawPRO ships loaned books to you at our expense, and you return books to us at your expense.

We have books on these topics:

- Billing & financial management
- Law firm management & administration
- Marketing & client relations
- Law office technology
- Career issues
- Wellness & balance issues
- Solo & small firm issues

For full descriptions of these titles, including downloadable tables of contents, go to practicepro.ca/library.