Law firms possess a tremendous amount of data on behalf of their clients. In order to improve mobility and reduce costs, this information is often stored in such a way that it can be accessed remotely via the Internet. While the ability to access data remotely provides many benefits, it also poses the risk of a data breach. In 2016, the American Bar Association reported that over twenty-five percent of firms with more than 500 lawyers experienced a data breach. The ubiquity of breaches, the large amount of private information safeguarded by law firms, and the rules and opinions of state bars require that lawyers review their ethical and professional obligations while embracing new technology.

Understanding Cloud Computing

As the Pennsylvania Bar Association succinctly explains, “cloud computing is merely ‘a fancy way of saying stuff’s not on your computer.’” Formal Opinion 2011–200 (quoting Quinn Norton, *Byte Rights*, Maximum PC, Sept. 2010, at 12). Rather, data is stored in a remote location, typically by a service provider. Some well-known examples of cloud-based applications include Office 365, Net Documents, Payroll, billing and HR software, Gmail, Skype, and Dropbox. These applications may hold all the important data of a law firm.

Applying Rules of Professional Conduct to Cloud Computing

Lawyers must use the cloud appropriately in order to fulfill their obligations to provide competent representation, maintain confidentiality, and safeguard client property. Comment 8 to Rule 1.1 of the Model Rules of Professional Conduct (the rule on competency) states that “a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology.” Thirty-one states have adopted this comment and the remainder will likely follow suit. Comment 18 to Rule 1.6 (the rule on confidentiality) lists several factors lawyers should consider when determining the reasonableness of their efforts to safeguard information. In addition to professional rules, some federal and state laws, such as the Health Insurance Portability and Accountability Act (HIPAA) also require the competent use of technology to safeguard information.

Currently, twenty states have issued ethics opinions on the use of cloud computing. While there is some variation among opinions, cloud computing is universally accepted, and even encouraged, so long as a lawyer takes reasonable care to ensure that data remains confidential and that reasonable safeguards are in place to protect data from breaches, loss, and other risks. “Reasonable care” is a flexible standard, likely chosen so that it can adapt with the ever-evolving nature of technology, but it provides little concrete guidance.

Taking Specific Steps to Fulfill Professional Responsibilities

Cybersecurity, a subset of information governance, has evolved significantly in the past few years. However, many firms still relegate cybersecurity to the IT department and provide little partnership oversight of the process. The policies governing cybersecurity are frequently drafted internally and not routinely updated to reflect new risks and prior events. Firms often do not pay sufficient heed to the risk their human capital poses to cybersecurity and are at risk from users clicking on malicious links or email attachments.
In light of these issues, many firms are now addressing cybersecurity, both for cloud stored data and for data hosted internally, in a more standardized manner. There are many existing standards such as ISO 27001, ISA, COBITT 5 and NIST SP 800-53. While the core functions of each policy have many specific guidelines for creating stronger and adaptive cybersecurity, there are a few elements that can specifically help with cloud-based computing. These are:

A. Use Strong Passwords

Hackers rely on victims reusing passwords and will attempt to use a cached password on other unrelated accounts; this type of attack is known as “credential-stuffing” and it is one reason that victims of the Yahoo data breach were advised to change the passwords to their non-Yahoo accounts. Lawyers should always select secure passwords and avoid reusing them. Passwords should contain a combination of numbers, symbols, and letters, and be at least twelve characters in length. They should also be changed regularly.

In addition to using complex passwords, many firms are also using two factor authentication. To authenticate to a computer people can use three elements: something they know (a password); something they have (a cell phone); or something they are (a fingerprint or face scan). Two factor authentication requires that you have two of these elements before authenticating to a server and accessing data. Many cloud providers now offer two factor authentication and any decision to not use it should be examined closely.

B. Encrypt Your Emails

Encryption rearranges data into code that can only be deciphered by using a decryption key. Data can be encrypted both while in motion (i.e. over the Internet), or at rest (i.e. on a desktop). Many larger firms have IT departments that provide the means to encrypt confidential data by sending it via a “secure” email. However, it is still incumbent upon the lawyer to work with the IT department to send an email by secure means when necessary. As of 2016, the ABA reported that only 26% of lawyers used email encryption when sending privileged and confidential documents to their clients. See ABA Tech Report 2016, David Ries, http://www.americanbar.org/publications/techreport/2016/security.html. Lawyers who work in smaller firms or solo practitioners should explore services that provide encryption. This could be as simple as encrypting the content in a Word attachment rather than sending it “in the clear” in the body of an email.

C. Be Vigilant of Scams

Human error is still one of the leading causes of data breaches. Hackers can gain access to information by using a variety of tools, including phishing scams and malware. Attorneys must remain mindful of these scams and never open or reply to an email, or social media message, from an unknown person. Lawyers should also avoid downloading risky apps or software and visiting suspicious websites.

Time and again, studies have shown that frequent training and awareness programs significantly reduce the likelihood of users falling victim to these scams. Many people attend training programs but then fail to implement what they were taught or feel that it does not apply to them. However, when associates realize the links they clicked could have compromised their firms, they are usually more receptive to future training!

D. Secure Your Device

Many firms currently have a bring your own device (“BYOD”) policy, meaning that lawyers are permitted to bring their own devices (i.e. phones and laptops) to the workplace and use them to access privileged data. If a lawyer’s device is lost or stolen, this could allow a third party to easily access the firm’s or clients’ information. As such, an attorney should secure his device by separating the firm’s sensitive information from the attorney’s own personal data on the device (known as “containerization”), installing antivirus software, and arranging two-factor authentication. Additionally, if working on an iPhone, an attorney can easily encrypt data by using a pin or passcode. Firms can implement policies on the phones before allowing them to connect that enforce these requirements and allow for remote wiping if the phone is lost or stolen. Lawyers should familiarize themselves with their firm’s BYOD policies and discuss security with knowledgeable people, such as the IT department, to ensure compliance.

Getting Your Head in the Cloud

Lawyers, our intellectual property brethren aside, typically struggle to understand and adapt to technological developments. In fact, our profession’s resistance to advancements in technology dates back to 1891, when lawyers lagged behind other trades using the telephone. See Behind Stables and Saloons: The Legal Profession’s Race to the Back of the Technological Pack, Mark Britton, 90-JAN Fla. B.J. 34 (2016). However, as cloud computing becomes increasingly common, and entire firms
become based in the cloud, lawyers can no longer let their aversion to technology risk the disclosure of confidential information. By employing simple techniques, lawyers can better serve their clients and fulfill their ethical and professional duties while taking advantage of cloud computing.

Jacqueline Cavallaro is an associate in the New York City office of Harris Beach. Her practice in New York and New Jersey focuses on defending pharmaceutical, medical device and supplement companies in product liability litigation. Ms. Cavallaro is the Vice-Chair of the DRI Young Lawyers Civility and Professionalism Subcommittee.

Alan Winchester helps organizations develop and implement compliance programs for critical information and systems, offering guidance on legal and regulatory requirements associated with the storage of protected information and what to do in the event of a data breach. He aids in developing and implementing information security incident response plans, and advises on how to work with IT professionals to investigate the scope of a data breach. Alan also represents organizations faced with either government investigations or private actions associated with cybersecurity loss.

To learn more about DRI, an international membership organization of attorneys defending the interests of business and individuals in civil litigation, visit www.dri.org.

© 2017 DRI. All rights reserved.