

September 2021

Paradigm

President's Podium:

New Milestones

**A New World:
Emerging from the COVID-19
Pandemic to Changed Workplaces,
Shifting Legal Practices and
New Friends**

Barton LLP is a mid-sized law firm, offering a full suite of services. At its core, we believe that innovation, agility and a commitment to value set us apart from the mélange of BigLaw firms that offer similar services.

Barton LLP

711 Third Avenue
14th Floor
New York, New York 10017

Tel: 212.687.6262

Kenneth N. Rashbaum
krashbaum@bartonesq.com

bartonesq.com

Primerus Member Since: 2016

Learn more at
primerus.com

Barton LLP New York, New York



What is the number one concern for clients and in-house counsel today? Security of clients' information handled by outside providers and the firm's overall cybersecurity safeguards have to be at the top of the list. As personal and private data are increasingly created, shared and stored electronically, the threats posed by cybercrime and regulatory investigations into alleged privacy and cybersecurity violations have never been greater.

Barton LLP is a mid-sized law firm, with offices in both New York and Nashville, whose purpose is to provide value, solve problems and foster opportunity. The firm consists primarily of former BigLaw partners who combine their extensive legal experience with Barton's flexible, value-driven service delivery model. Our senior attorneys work directly with clients on matters, taking the time to understand each client's business objectives

and long-term goals. We recognize that clients prioritize managing their resources and creating efficiencies — and they want lawyers who are able to do the same.

Barton offers a full suite of services, including in the areas of corporate transactions, litigation, financial services, tax services, real estate, family law, employment, cybersecurity, banking, immigration, intellectual property and emerging companies/venture capital, among others. At its core, we believe that innovation, agility and a commitment to value set us apart from the mélange of BigLaw firms that offer similar services. Our business model is designed to foster collaboration between attorneys, while providing them the autonomy to grow their practices and streamline interactions with clients.



Kenneth N. Rashbaum

Kenneth N. Rashbaum is a partner with Barton LLP in New York City, where he heads the privacy and cybersecurity group. He is also an Adjunct Professor of Law at Fordham Law School in New York. Barton's cyber compliance team is offering Primerus firms a multi-step information security initiative at a discounted flat fee which comprises an evaluation of the firm's compliance with industry standards for cybersecurity; baseline client security requirements for law firms; confidentiality and privacy laws and regulations such as General Data Protection Regulation (GDPR), HIPAA and California Consumer Privacy Act (CCPA); and certain financial services regulations that clients use to determine whether to engage law firms.

Law Firm Cybersecurity: How Firms Can Meet a Top Concern for Clients and Their In-House Counsel, Get New Business and Retain Existing Business

Security and integrity of a client's information shared with and maintained by their law firms, along with the firm's overall cybersecurity safeguards, can make the difference between gaining/retaining business and losing business. Firm compliance with legal and regulatory standards for data protection (privacy plus security) is something that an increasing number of clients rely upon to qualify their law firms, often incorporating company, legal and industry standards into their guidelines for use of outside counsel.

Management of law firm third-party risk occupies a great deal of space in outside counsel guidelines — and for good reason. Cyber-attacks and data breaches in which intruders gained access to clients' confidential and proprietary information are in the news on a regular basis. Several U.S. law firms, as well as academic research institutions, were recently targeted by cyber-criminals who accessed data that was stored with a third party, Accellion. The New York City Transit Authority was attacked in the spring of 2021 through a weakness in the third-party platform that it used to authenticate employees and contractors who needed access to the Transit Authority's database. Going back further, the breaches of Target and Home Depot occurred when hackers infiltrated their systems through weaknesses in the networks of subcontractors, including an HVAC contractor in the case of Target.

Law firms have ethical responsibilities to protect the confidentiality of their clients' communications through, among other things, monitoring their third-party business partners and vendors who have access to the firm's data. This responsibility includes oversight of third-party email and other platforms operated by third parties to assure that they can and do assist the firm in meeting the ethical duty to maintain confidentiality of client information. Client outside counsel guidelines comprise requirements for selection due diligence, supervision and audit (under certain circumstances) of third parties who host client information.

Laws and regulations such as HIPAA, the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the New York SHIELD Act also require that entities covered by these schemes that engage third parties (including law firms) to host or access protected information, exercise and document due diligence into the third party's security safeguards. Law firms, as third-party processors or service providers to entities covered by these schemes, are explicitly within the ambit of third-party requirements. For example, GDPR, CCPA, HIPAA, the New York SHIELD Act of 2019, and the Cyber Security Regulations of the New York State Department of Financial Services (which supervises all organizations authorized to do business in New York pursuant to the Banking and Insurance Laws)

require that entities conduct and document due diligence into the cybersecurity safeguards of third parties, including law firms, before engaging them. In addition, these entities must represent and warrant in their engagement agreements that they can and will need explicit information protection safeguards regarding cybersecurity and privacy in third-party service agreements.

Primerus member law firms therefore have legal, ethical and business requirements when it comes to hosting confidential client information, as well as when selecting and retaining third parties who will also have access to this information. Yet, small and mid-sized firms like those in Primerus may find that the resources to meet these emerging client requirements for cyber compliance are daunting. Much larger firms with seemingly unlimited resources have been successfully attacked, with information about and created by their clients disclosed. So what hope is there for firms like ours? The answer lies in working with the right advisors and using the right process. In this way, our firms can successfully meet client, legal and ethical standards without incurring the significant costs of many standard commercial cybersecurity programs.

Law firms are not banks, hospitals or e-commerce platforms. They create and use electronic information differently but are bound by many of the same legal standards



as their clients in regulated industries. The cybersecurity assessment process should be facilitated by advisors who are also lawyers and understand the landscape of law firm data access uses, storage and disclosures. These advisors can work with the law firm to propose a cybersecurity assessment initiative and protocols for protection of law firm information that won't interfere with the firm culture or the work of attorneys. Rather, in addition to meeting client, legal and ethical standards, effective cybersecurity protocols would also have the benefit of creating efficiencies in the uses of information.

The elements of a process that would fit most Primerus law firms are as follows:


- **Preparation of a Data Map:** A firm cannot protect its clients' information if it doesn't know all the places that information resides. This sounds, to paraphrase the great detective Sherlock Holmes, elementary, but let's dig a little deeper. In the COVID era, but also well before it, lawyers worked from the road and their homes. So firm data may be on their phones, laptops, tablets or home computers. How is it secured in each

place and in transit from those places to the firm's servers? What third parties have access to that information, including such business partners as email system providers, human resources platforms, and outside IT providers?

- **Third-Party Risk Management:** Do these third parties represent and warrant that they will keep your information at least as confidential and secure as you do? How can you monitor them to assure that they continue to do so? Remember, the firm is responsible for data it entrusts to third parties.
- **Remote Access:** In the COVID work-from-home area, the target environment for hackers became much richer. Your advisors should work with you to assure your safeguards for accessing the network remotely are in place and are standard in the industry.
- **Update the Security Protocols:** When are security patches installed? The 2021 attack that hit on-premises Microsoft Exchange servers obtained law firm data mostly from those firms that had not installed the patch that Microsoft had published well before the attack.
- **Testing the Network:** Your advisors should obtain "white-hat" or "ethical"

hackers who will attempt to break into the firm's system and then provide a report (preferably through cybersecurity counsel) as to weaknesses they found and how best to remediate them, making sure they document that remediation.

- **Policies and Procedures:** How will your attorneys and staff know what they should and should not do? What will various clients require of the attorneys and staff for protection of their data? Policies and processes, written in plain English by advisors who are also attorneys and speak your "language," will leave little room for uncertainty concerning firm cybersecurity protocols.
- **Attorney and Staff Training:** Prepared by lawyers for lawyers, these documented interactive sessions can educate the work force on how and why cybersecurity is the concern of the entire firm, not just the information technology department.

In this way, your advisors can provide you with a baseline of cybersecurity compliance benchmarks so that you can meet client expectations, attorney ethical standards, and legal requirements for confidentiality of client information. 

Primerus Member Firms Globally

125

North America Region

22

Europe, Middle East &
Africa Region

8

Asia Pacific Region

16

Latin America &
Caribbean Region



P PRIMERUS

The World's Finest Law Firms

International Society of Primerus Law Firms

452 Ada Drive, Suite 300
Ada, Michigan 49301

Tel: 800.968.2211 (toll-free)
Fax: 616.458.7099
primerus.com

*The International Society of Primerus Law Firms
finds and accepts only the finest independent law
firms and lawyers.*