Dear Reader,

Thank you for your interest in this whitepaper.

Based on what our firm is seeing in the legal industry, the issue of cyber security risk is top of mind for the leaders of many law firms. In working with law firm executive leadership and administrative staff across the industry, we’ve gained insights about the challenges law firms currently face related to the security of their information technology.

As our whitepaper will discuss in the following pages, these challenges are wide-ranging and may be difficult to overcome based on the resources many firms currently have available. We hope that the solutions and perspectives discussed in this publication will assist you in making your firm’s information technology more secure for your professional staff and clients.

Regards,

RubinBrown’s Law Firms Services Group
Law firms are being targeted by cyber criminals at an ever-increasing pace. Some of the country’s most prestigious firms have found themselves in the headlines because hackers exploited weaknesses in their information systems.

Sensitive client information, which was provided to these firms under the assumption that it would be held in trust, was exposed and possibly used for illicit purposes. Situations like these have caused firms to be subject to more scrutiny with regard to how they safeguard their clients’ and prospective clients’ information. Clients have responded by subjecting their legal providers with swarms of checklists, revised engagement letter terms, disclaimers and on-site visits by their own auditing and security professionals.

Validating security is becoming a requirement prior to obtaining and for retaining a client.

The cyber security issues in the legal marketplace have impacted the most sacred responsibility that attorneys have with regard to their clients: the attorney-client privilege.

“A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”

- ABA Model Rule of Professional Conduct 1.6 (c), Confidentiality of Information

The constant threats related to law firms’ information security are real and the marketplace has responded in various and unpredictable ways to verify information will be safe with their lawyers and that the attorney-client privilege will be upheld. Requests to verify firms’ information security systems have been persistent and, in many cases, resulted in significant burdens on firms’ information security personnel.

However, there is an option available to minimize the time spent on these activities while making firms’ security stronger to enhance trust with their prospective and current clients. One of these options is defined by the American Institute of Certified Public Accountants (AICPA) through an attestation engagement in order to provide an opinion on the internal controls at service organizations, such as law firms.

The purpose of this whitepaper is to provide more information on these types of engagements and why they would be ideal for law firms operating in the environment where the focus on information system integrity is intense.
Current State of Law Firm Cybersecurity

Clients and prospective clients have requested law firms to agree to additional contractual content and representations related to security and to be subjected to on-site reviews of their IT security controls, systems and processes. When considering that some law firms may have many clients with their own individual concerns regarding their firms’ IT structure, these requests for additional information can become burdensome.

When handling multiple requests, the time incurred to meet the demands of each request can become excessive. As a result, law firms are seeking solutions to test their information security systems thoroughly and then document once to distribute the results of these procedures in a uniform and clear manner.

Further, an issue that law firms struggle with is, once certain levels of security, system availability, confidentiality and privacy are attained, how can they objectively measure the results of their compliance efforts? To address this, criteria can be developed and evaluated by independent auditing and security firms, and includes elements such as the design and operating effectiveness of relevant IT controls. Conducting these activities represent a key opportunity to ease the effort related to a very important element in a law firm’s information security process.

By obtaining the objective opinion of an independent auditing and security firm, clients and prospects of law firms can obtain even more assurance regarding a firm’s security systems. Based on the current conditions facing law firms, an attestation engagement designed to test controls of IT security conducted by an objective auditing and security firm may assist in:

- Alleviating the concerns from clients and prospects
- Saving law firms valuable time
- Providing additional comfort to executive partners and the board of directors

Law firms provide legal services to their clients and obtain, process and report on confidential information for their clients. A service organization is defined by the AICPA as “an organization, or segment of an organization, that provides services to user entities.”

The AICPA provides standards, guidance and related peer review programs to help ensure the quality of attesting on security for service organizations such as law firms. In such an engagement, the controls identified by the law firm for their relevant IT security processes are evaluated for design and operating effectiveness, over a period of time. Conducting an attestation engagement provides an opportunity to effectively test and document areas and provide a report on the results of the test in a single summarized format. This is in contrast to testing and reporting in a redundant fashion that is currently the trend within many law firms.
What is a Service Organization Controls (SOC) Report?

Service organization controls (SOC) reports are designed to help service organizations build trust and confidence in their service delivery processes and controls through a report by an independent certified public accountant with security expertise. Each type of SOC report is designed to help service organizations meet specific user needs.

When users of a service organization’s services (user entities or clients) outsource certain tasks and functions, many of the risks of the service organization become risks of the user entities. In light of high-profile internal control break-downs and heightened focus on IT security throughout the legal marketplace, law firm management is focusing more on enhancing IT security control activities. By engaging an independent CPA to examine and report on law firm’s controls, law firms can respond to meet the needs of their clients and obtain an independent evaluation of the effectiveness of controls that address cyber security activities.

There are three levels of SOC reporting options:

**SOC 1 Reporting** – Reports on controls at a service organization relevant to user entities’ Internal control over financial reporting.

**SOC 2 Reporting** – Reports on controls at a service organization relevant to security, availability, processing, integrity, confidentiality and privacy.

**SOC 3 Reporting** – One of the primary differences between a SOC 2 report and a SOC 3 report is a SOC 3 report is a general-use report that provides only the auditor’s report on whether the system achieved the trust services criteria (no description of tests and results or opinion on the description of the system).

The Three Levels of SOC Reporting Options

- **SERVICE ORG CONTROL 1 (SOC 1)**
  - SSAE16 - Service auditor guidance
  - Restricted Use Report (Type I or II report)
  - Purpose: Reports on controls for F/S audits

- **SERVICE ORG CONTROL 2 (SOC 2)**
  - AT 101
  - Generally a Restricted Use Report (Type I or II report)
  - Purpose: Reports on controls related to compliance or operations

- **SERVICE ORG CONTROL 3 (SOC 3)**
  - AT 101
  - General Use Report (with a public seal)
  - Purpose: Reports on controls related to compliance or operations

Trust Services Principles & Criteria*
Focus on SOC 2 Reporting for Law Firms

The procedure that a law firm goes through in order to receive a SOC 2 certification over its information security system requires a review of the following key areas:

- Infrastructure
- Software
- People
- Procedures
- Data

The SOC 2, Type II verification (which includes testing of operating effectiveness) consists of an independent examination of a law firm’s internal control for security and/or other trust principles, over a specified period of time, usually 6 months to a year.

The means by which a firm’s systems are independently tested for SOC 2 purposes should be conducted by the standards prescribed by the AICPA. Note, the SOC 2 (referred to as a SOC 2+) maybe mapped to standards such as ISO 27001 (for more information, visit www.iso.org).

The process will result in a SOC 2 report for a law firm to distribute to user entities (clients and prospective clients) and a logo for the law firm’s website. Obtaining a SOC 2 report, which is unqualified, assists attorneys in upholding the attorney-client privilege. Additionally, insurance carriers’ requirements of maintaining protocols over information security can be satisfied with a SOC 2 report. Independent opinions on a firm’s security controls allow for clients to trust that their information is being handled in a manner that is safe and private.

Finally, firms currently find themselves being required to respond to requests regarding information security based on individual concerns, thus creating a redundant process within a firm’s IT group.

Once a firm achieves SOC 2 certification, the SOC 2 reporting mechanism is designed in such a way that allows firms to test their systems once and report many times over to clients and other parties inquiring about a firm’s security. A SOC 2-compliant firm could issue a SOC 2 report upon request to those making inquiries about a firm’s information security. While the first year to achieve SOC 2 certification can be time-consuming, achieving certification in subsequent years is much less time intensive.
Instilling Trust in Clients with Regard to Their Data

The need for clients to trust that their sensitive data is safely and securely maintained by advisors has never been more critical. Companies with cyber security breaches seemingly make headlines on a daily basis. A law firm should be taking steps with regard to information security in two forms: prevention of breaches and response to data breaches should they occur.

By following the trust principles set forth by the AICPA, SOC 2 reporting represents an opportunity to obtain assurance from an independent accounting firm regarding security, availability, processing integrity, confidentiality and/or privacy over IT. Also, as a result of the process, a firm will gain valuable insights into how information is maintained, secured and managed throughout the organization.