ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Implement the Data Steward Program to Protect Your Data

Compliance and Ethics

Technology, Privacy, and eCommerce

Banner artwork by Good_Stock / *Shutterstock.com*

Cyber-attacks on law firms and other legal service providers continue to rise year-over-year, and with them, costly data breaches. Your company has made significant investments in its own security game, and now is focusing on service providers with whom your company shares sensitive financial, business, and customer information. But vetting vendors is hard work. **How can your organization ensure law firms and legal service providers are keeping your data safe**, without overburdening these key business partners or expending undue resources?

This two-part case study, undertaken by law firm Kutak Rock LLP in cooperation with the ACC, answers that question.

The problem for in-house counsel

In 2019, ACC surveyed in-house counsel to determine their capabilities for assessing law firm data security. Fully 70 percent had no solution in place. And of the remaining 30 percent, one-half assessed their firms only at onboarding or “as needed,” and the other half assessed their firms every one to three years. Two-thirds of both segments wanted to implement a new or improved solution.

Two years later in a follow-up survey, ACC found that legal departments had not moved the needle: 70 percent still had no solution in place, and 30 percent were still unsatisfied with their current solution. A supermajority said that solving this problem is an urgent priority.

Which raises the question: **What are your options as in-house counsel** — and the challenges — for implementing a mechanism to assess and manage the security of data that you share with law firms and legal service providers?

1. **Outside counsel cybersecurity guidelines** — One common strategy is to add data security provisions to outside counsel guidelines. This approach can be effective in giving your law firms direction, and can be updated from time to time to meet emerging cyber risks. The primary challenge, however, is that most legal departments don’t perform any due diligence to determine whether these provisions are being met, and therefore have **no visibility** into their firms’ compliance with the guidelines. (At least not until they receive notification of a data breach.)
2. **Independent security audits** — An increasing number of law firms and service providers have retained independent experts to audit their security posture under ISO 27001, SOC 2, and similar security standards. These programs can give you, the client, assurance that the audited firms are committed to ensuring data security. But typically, only a **small percentage** of your firms will have engaged in such an audit program. And the audit reports often provide **limited visibility** into the systems and controls that were subject to audit. Your corporate information security team will typically require additional information via their own security audit or questionnaire.
3. **Corporate security audits** — Rather than rely on law firms to initiate their own independent audits, your information security team can conduct the audits themselves. That way you can be sure all of your law firms and service providers are assessed equally, and you will have complete visibility into audit results — including any concerns that require remediation. Nevertheless, conducting audits can be **extremely labor intensive**, and therefore they are typically used only in exceptional circumstances — such as one-time onboarding of a new law firm or vendor, or prior to sharing data in a particularly sensitive matter.
4. **Self-assessment questionnaires** — By far the most common method used by companies to assess third-party data security is to send their vendors a self-assessment questionnaire. This allows the information security team to ensure all of the company’s questions are included in the assessment, and all of the company’s vendors are asked the same questions. That said, this method too is quite **labor intensive** — developing and maintaining a comprehensive questionnaire; identifying vendors and contacts; sending, pursuing, and evaluating completed questionnaires; and monitoring vendor remediation. As a result, in a rapidly changing cybersecurity landscape, only **29 percent of companies assess** the security of even their highest-risk vendors — those with access to sensitive and confidential information. And they do it **just once every 1-3 years**.

Self - assessment questionnaires remain as one option that is least effective and too time consuming for in-house counsel to ensure the safety and security of data. FAHMI98 / *Shutterstock.com*

> By far the most common method used by companies to assess third-party data security is to send their vendors a self-assessment questionnaire.

The problem for law firms

Law firms recognize they are generally high-risk service providers. Companies provide extremely sensitive legal information to their law firms and vendors which, if breached, poses a

material threat. Cybercriminals are increasingly attacking law firms to gain access to this sensitive client data. Attorneys and their firms also have both a pre-existing duty of confidentiality dictated by the Rules of Professional Conduct, and concurrent privacy and security obligations under various statutes and regulations. So, the circumstances in which firms obtain and share confidential information are quite different from corporate IT, customer service, marketing, supply chain, or other vendors.

From a law firm perspective, the net result is an ever-increasing **barrage of one-off questionnaires**, sent by clients who understandably are trying to implement some degree of security due diligence for all of the firms on their panels. For law firms, this has become a **frustrating drain on resources** better spent on implementing active security measures. A few of those frustrations include the following:

- While virtually all vendor-vetting questionnaires derive from the same collection of industry-standard security requirements, each **articulates its questions somewhat differently**, necessitating time-consuming, individualized responses.
- The majority of questionnaires are omnibus documents directed to **all vendor types**, and not specifically customized for legal services. Many of the resulting questions range from irrelevant to impossible for law firms to answer. And simply marking the questions “N/A” is unacceptable.
- In-house counsel **rarely have the technical resources** necessary to interpret and evaluate law firm technical responses. As a result, the questionnaire responses often amount to just paper exercises “for the record” — rather than encouraging dialogue about ways to improve client support.
- Many of the largest companies **outsource the vetting process**. While this may be effective for generic customer service, marketing and supply chain vendors, law firms almost always experience negative results that lead to low response rates. Outsourced processes typically fail to account for the unique attributes of legal service providers and the ways they receive, share, and use data. This can be costly, time-consuming, and unsatisfactory to both in-house counsel and their providers.
- Questionnaires are implemented on platforms that generally range from poor to awful, with clunky interfaces and **“black box” scoring** mechanisms — with technical support contacts ranging from offshore consultants to in-house, IT, or third-party risk management departments.

In competitive situations, the litany of drawbacks outlined above may force a law firm to conduct a cost-benefit analysis to determine whether “the juice is worth the squeeze.”

Small firms may take a pass on new work not because they are unqualified — but to avoid sinking time into lengthy or impossible questionnaires or security audits. Larger firms may decline one-off questionnaires and simply present their security credentials for companies to assess as best they can.

In-house counsel may be forced to disqualify a firm they would like to retain because the firm cannot easily clear the security evaluation. Clearly, none of these outcomes is optimal for either party.

The ACC Data Steward solution

Assessing and evaluating law firm security is a difficult, cumbersome, and resource-intensive process, both for companies and their law firms. The ACC board of directors saw an industry-wide need for a smarter, more efficient and effective approach, and authorized development of the Data Steward Program (DSP) to meet the need.

From the outset, ACC decided it was crucial to develop the solution through industry collaboration in three committees: a Controls Committee for technical decisions, a Working Group responsible for program design, and an In-house Advisory Board for final vetting and acceptance. Committee members represented a wide variety of perspectives, including in-house counsel, CIOs, CISOs, cybersecurity attorneys, and other information security professionals from corporate legal, law firms, and legal service providers.

Data Steward is now a mature program, giving in-house counsel a tool for assessing and benchmarking their law firms, and giving the firms a tool for demonstrating their capabilities. The resulting solution addresses key in-house and law firm requirements as follows:

- **Controls** — The ACC Data Steward Program utilizes **industry-standard information security controls**, mapped to and drawn from global standards such as NIST 800-53 and ISO 27001, widely recognized as authoritative by both in-house and law firm security experts. The controls were also customized for the legal industry: Selected to ensure client data security at all law firms and legal service providers, large and small; edited to avoid "open-ended" questions that require an essay in response; and formatted into discrete, scoreable "yes/no" requirements. The result is a Core Assessment questionnaire consisting of 42 questions addressing plus controls, and widely vetted and accepted as the emerging legal industry standard. **In-house counsel no longer need to develop and maintain their own one-off questionnaires.**
- **Dashboard** — Upon completing the DSP self-assessment, law firms can give their clients access to view the results in the **DSP Dashboard**. In-house counsel can use the Dashboard to compare and contrast results of all of the firms on their panel. And they can drill down to see details for any particular firm. Those details include an overall score from 0-100 percent; the systems and locations covered by the assessment; and non-compliant issues that may prompt a request for remediation. The simplicity and transparency of the Dashboard allows technical and non-technical team members to review results at a high level or more in depth, as appropriate. Law firms, on the other hand, can use this single questionnaire to demonstrate their security profile to all of their clients. **Law firms no longer need to complete their clients' one-off questionnaires.**
- **Cloud software platform** — ACC has implemented Data Steward on AuditBoard, the leading SaaS platform in use by internal audit departments. The software allows law firms to **update their profiles in real-time** — whenever they remediate a control that has been non-compliant, their score will improve and clients will see it. In addition, the software provides secure audit workspaces where in-house counsel can validate a firm's self-assessment, based on supporting evidence. Law firms in turn can create a secure evidence repository, and simply clone the evidence into a new audit workspace whenever a client requests it. **The entire audit process is remote, efficient, and secure.**

Cloud software platforms such as AuditBoard allows for an easier and more successful approach to assessing law securities. AB Graphic / *Shutterstock.com*

Compared to the cost of completing multiple one-off questionnaires, the investment to purchase a DSP platform license and become DSP Accredited is a bargain.

- **ACC Accreditation** — Firms that complete the DSP self-assessment can elect to add independent validation of their score (and documentation) by an ACC-Accredited Assessor, with the opportunity to become “ACC Accredited.”Prior to adopting Data Steward, Kutak Rock’s standard security package was highly technical, loaded with terms such as ISO 27001:2013, SIG-Lite, ISMS, and AES 256-bit encryption. These are meaningful terms to security professionals, but difficult for someone in the legal department to interpret. With ACC Accreditation, however, Kutak Rock clients can rely on the fact that an independent assessor has examined and approved Kutak Rock’s evidence for compliance with the DSP controls. Law firms with mature information security programs who score well on the self-assessment should have no hesitation about submitting to an independent audit to validate their DSP results. Compared to the cost of completing multiple one-off questionnaires, the investment to purchase a DSP platform license and become DSP Accredited is a bargain.

Kutak Rock’s strategy for client adoption of Data Steward

ACC interviewed Elise Dieterich, Kutak Rock’s Information Security & Privacy Counsel, overseeing client assessments. Kutak Rock joined the Data Steward Program (DSP) at a client's request, impressed by the tailored DSP self-assessment for law firms and the ease of sharing via AuditBoard. They became early ACC Accredited supporters.

Kutak Rock values ACC's outreach to its 45,000 members and 10,000 organizations, promoting DSP for assessing law firms' security. Unlike conventional vendors charging fees, ACC offers in-house counsel free access to the DSP platform and law firms' security profiles. ACC believes the cost of security assurance should be on the party seeking business, not the client. A low-cost DSP license enables law firms to create self-assessment scorecards, share with clients, host remote audits, and track remediation efforts.

The distinction lies in the rollout approach. Legal departments can easily implement DSP across their panel, ensuring a standardized assessment. For law firms, DSP is a one-off questionnaire until clients widely adopt it. Kutak Rock aims to promote DSP adoption among its clients, leveraging its time and cost-effectiveness.

Despite previous disappointments with platforms promising broad leverage, Kutak Rock is optimistic about ACC's success. Factors include ACC's extensive membership appeal and DSP's purpose-built design addressing long-standing legal sector challenges. Unlike other platforms, DSP uniquely focuses on providing tailored assessments for the legal sector's specific attributes.

Case study, Part 1

Having achieved ACC Accreditation, Kutak Rock is now planning to reach out to its clients and, with the assistance of ACC, to persuade them to ratify Data Steward Program as an acceptable platform for security assessments.

Dieterich explains that the goals are twofold: For clients who have expressed a desire to confirm that their data is secure at Kutak Rock, but have not yet instituted a formal assessment program, the ACC Data Steward Program offers an effective way to view their law firm’s security profile and provide needed assurance. And, for clients that currently use one-off assessment mechanisms, the Data Steward Program provides an opportunity for greatly improved efficiency.

Hopefully, these clients will see the benefit of allowing Kutak Rock to transition firm resources away from slogging through one-off questionnaires, to completing value-add security projects. For a firm with thousands of active clients, virtually all of whom are interested in verifying Kutak Rock’s security bona fides, Data Steward’s one-to-many model is an obvious game-changer.

In Part 2 of this case study, in a future *Docket* article, we will report back on the success metrics, barriers to success, next steps, strategies, and conclusions we have drawn from the project. We expect to identify key issues and metrics such as the following:

Phase 1: Law firm planning

- Gaining executive level support for reaching out proactively to clients about data security;
- Synchronizing client outreach with the firm's marketing efforts;
- Addressing relationship partner concerns, overcoming barriers, and formulating individualized messaging; and
- Identifying types of clients to be excluded from the project, if any.

Phase 2: Clients who today send outside counsel guidelines with cybersecurity provisions

- Percentage of clients that send outside counsel guidelines;
- Percentage that include cybersecurity guidelines;
- Percentage of clients that follow up to assess compliance;
- Anecdotal reactions to Kutak Rock outreach, compliance results and ACC Accreditation; and
- Percentage that indicates willingness to accept Data Steward for assessing compliance.

Phase 3: Clients who today send assessment questionnaires

- Percentage of clients that send security assessment questionnaires;
- Percentage that also send cybersecurity guidelines;
- Common issues and barriers to completing questionnaires accurately and timely;
- Types and prevalence of questionnaire platforms, and impact on duration to completion;
- Types and prevalence of points of contact, and impact on duration to completion;
- Percentage of clients who generate follow-up questions, or requests for remediation;
- Anecdotal examples of effective and ineffective question types and platforms;
- Anecdotal reactions to Kutak Rock outreach, compliance results, and ACC Accreditation; and
- Percentage that indicates willingness to accept Data Steward for assessing Kutak Rock compliance.

Phase 4: Clients who today do not assess their law firms' data security profiles

- Percentage of total clients who do not assess;
- Anecdotal reactions to Kutak Rock outreach, compliance results, and ACC Accreditation; and
- Percentage that indicates willingness to adopt Data Steward for assessing KR compliance.

The authors welcome any comments you may have on other issues to test; similar information available from other case studies; or suggestions for topics to cover in the next article, Part 2.

James Merklinger

Chief Advisor

ACC Credentialing Institute

James A. Merklinger oversees the institute In-house Counsel Certification Program and its Data Steward Program, assessing law firm data security practices. Having served ACC for over 20 years in a variety of key roles, Merklinger was named to the position of president of the ACC Credentialing Institute in 2017. In this role,

he is responsible for establishing standards and advancing ACC's ability to establish an in-house counsel credentialing program. Merklinger is also responsible for leading the ACC Data Steward Program to evaluate the security profile of law firms.

Previous to his role as the Institute's president, Merklinger served as ACC's vice president and chief legal officer. He represented ACC on all legal issues affecting the association, including mergers with the Australian Corporate Lawyers Association , the Hong Kong In-house Counsel Association and the Corporate Counsel Middle East. Merklinger advised the organization on meeting the needs of the in-house counsel community. He had also served as ACC deputy general counsel and vice president - legal resources, overseeing the development of ACC's array of resources to help in-house counsel do their jobs. In this position, he worked with 18 volunteer leadership committees, organized by practice areas, which contribute to the strategic development of the association's resources and education programs. Merklinger spearheaded ACC's regular benchmarking studies to provide members and the legal industry at large with key trends related to the in-house counsel practice and outside counsel management.

In addition to his non-profit legal experience, Merklinger served on the board of directors for the Tourette's Syndrome Association of Greater Washington, DC, the board of directors of the ACC Foundation, and President of the Washington Irish. Prior to joining ACC, he served as in-house counsel for DIAD, Inc. in Reston, Virginia. While at DIAD, he provided counsel in a variety of substantive areas, including commercial law, software licensing, disability law and issues affecting entrepreneurial development. Merklinger has served as faculty for CLE programs throughout the United States, Canada , Europe and the Middle East on a variety of in-house topics. Merklinger graduated from Wofford College and the University of South Carolina School of Law.