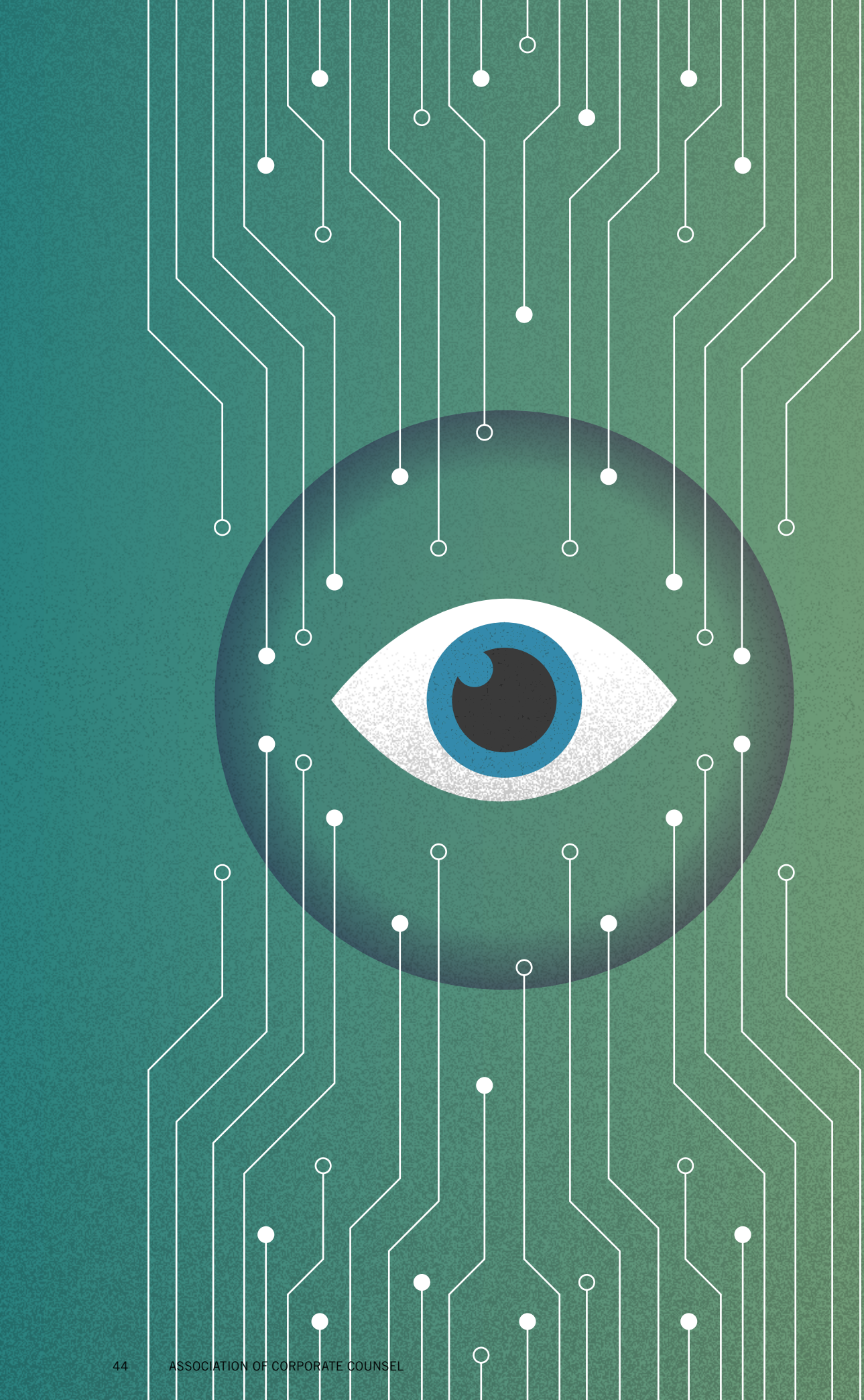

CHEAT SHEET

- *Under attack.* Client data held by law firms is increasingly subject to attacks. Yet in-house counsel often lack the processes, skills, and resources to determine if their law firms are appropriately protecting and managing their companies' most sensitive information.
- *Reputational risk.* This is a problem not only for in-house counsel, but also for law firms as they find it increasingly difficult and cumbersome to demonstrate to their clients and prospects that they are effective data stewards.
- *Score once, share widely.* The newly launched ACC Data Steward Program is a cross-industry collaboration between in-house counsel, law firms, and other key stakeholders in the legal industry that has developed a framework of accepted industry standards for protecting legal information. The program provides law firms an "answer once, share many model," in which they can go through a detailed scoring process once, and then leverage this many times for new and existing clients.
- *Industry standard.* The ACC Data Steward Program will collaborate across the industry, monitoring new threats, updating controls and sharing best practices, and raising security capabilities across the entire legal industry.

INTRODUCING THE ACC DATA STEWARD PROGRAM

The Easiest Way to Ensure Law Firms Have the Ability to Protect Sensitive Information

By Paul Danna, James Merklinger, and Michele Shuster

Cybersecurity and data protection are among the biggest concerns for all enterprises today. The news is filled with reports of data breaches causing economic and reputational harm. Businesses struggle to cope with the risk of data hacking and breaches while dealing with the pressures of governance and regulatory requirements.

Take Epiq Systems Inc., which caters to top law firms, investment banks, and industrial conglomerates by helping them sort through digital records for compliance and restructuring. In February 2020, the company was attacked by hackers. Epiq took its systems offline to limit outside access and safeguard client files. This led to litigation delays as clients couldn't access critical documents. This episode illustrates the wide-ranging effects of hacking, even unsuccessful attempts.[1]

No group is more impacted by concerns about sensitive data than corporate counsel. These individuals are concerned not only for the security of data that is directly under corporate control, but also for the safety of sensitive legal information shared with their law firm, eDiscovery vendors, and other legal services partners. With the *ABA TECHREPORT* 2019 reporting that 26 percent of all independent law firms surveyed have suffered a data security breach in the past year, and an additional 19 percent of survey respondents having honestly reported that they did not know whether a breach has occurred, it is not surprising that corporate counsel are asking their legal partners: "Is my data secure?" Whether a cybersecurity event is reported or not, the events will continue to occur.

It's hard to know if legal information is protected

Driven by this concern, in-house counsel have increasingly sought ways to better understand the data security and governance practices in place at law firms and legal service providers. Many legal clients have sought this information by developing their own unique data security questionnaires. These surveys or audits generally are comprised of 50 to 500 or even 1,100 questions, often pulled from a variety of information security frameworks that were not built to address the legal service environment. The time it takes for companies to develop and publish the questionnaires, and for law firms to review and respond is significant. Once these questionnaires are completed, evaluating the responses is difficult at best. Corporate IT/Infosec staff — who are often called upon to administer the review — often write the questions using technical jargon, do not understand the legal practice, and cannot interpret the answers with relevance to specific practice areas or matters.

Furthermore, if in-house counsel wants to bid a project across multiple law firms, it is difficult for them to get their security teams to review all the responses. In a survey conducted by ACC last year, more than 70 percent of ACC members do not evaluate the security and governance capabilities of their legal services providers. In-house counsel need a better approach.

"We take the data security of the information we provide to law firms very seriously," says Shawn Cheadle, general counsel of operations at Lockheed Martin Space and co-chair of the Data Steward In-house Advisory Board. "Companies need an easier and more practical way of evaluating their law firms."

No one likes the current process, law firms, and eDiscovery vendors included

From the perspective of law firms, the lack of a standard framework of best practices for information security makes it difficult to benchmark against

ACC Foundation's 2020 State of Cybersecurity Report

More than 1,000 chief legal officers answered a cybersecurity survey conducted by ACC.

- CLOs ranked data privacy and cybersecurity as the second most important issue for their organization (only behind regulatory compliance).
- CLOs were asked about any new issues that the board of directors has been asking them about in an open-ended question, and cybersecurity, risk, and compliance were the top three issues that board members asked CLOs about.

According to the *ABA TECHREPORT 2019*, 26 percent of all independent law firms surveyed have suffered a data security breach in the past year, and an additional 19 percent of survey respondents reported that they did not know whether a breach had occurred. Privacy and cybersecurity were the second most important issue for their organization (behind only regulatory compliance).

Paul Danna is a May 2020 graduate of the Charleston School of Law. He currently works at the Office of Information Assurance of the South Carolina Department of Health and Human Services. He is a member of the association for Data and Cyber Governance, CyberSC, and Information Technology Professionals of South Carolina. *pdanna@charlestonlaw.edu*

James Merklinger is the president of the ACC Credentialing Institute. *merklinger@acc.com*

Michele Shuster is a founding partner of Mac Murray & Shuster where she works with consumer-facing businesses in highly regulated industries nationwide. *mshuster@mslawgroup.com*

a defined goal or other firms in the industry. Without such benchmarks, it is challenging to set investment priorities. To address this gap, some law firms have chosen to invest heavily in achieving an industry-standard certification (such as ISO 27001). But the scope of an ISO certification can be very broad, and the investment is not affordable for all firms.

But the alternative — responding to individual questionnaires — is not satisfactory either. This approach does not guide the firm's internal priorities or enable the firm to benchmark itself against others in the legal industry. As a partner in one law firm admitted: "I don't know what good is." Moreover, it is labor-intensive and time-consuming (often described as "spreadsheet hell") to respond to the ever-increasing number of unique information security and governance questionnaires provided by each client. This consumes significant resources — the very resources that would be better spent securing client data.

Even after the questionnaires and associated evidence are completed — despite many efforts by both in-house counsel and law firms — both sides often do not have a clear understanding of the status and issues. Unlike data security standards for financial services, for example, the legal profession does not have a basic set of rules for information security and information governance. This is a problem because most law firms install some level of cybersecurity, but the level of security varies without a clearly defined minimum level for information security and information governance. In-house counsel remain unsure that their legal information is being properly managed while law firms are frustrated at the increasing amount of valuable resource they are investing to demonstrate that they have the right controls in place.

ACC is addressing these issues with the launch this fall of its Data Steward Program for Assessing Client Information Security and Governance. Utilizing a collection of industry standard controls, including National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO) controls customized for the legal industry, this voluntary program invites law firms and legal services providers to be scored on their data security controls and governance processes for client legal data. Additionally, the program offers an accreditation option in which independent third-parties assess law firms' capabilities and ensure that they are meeting the required security levels. The firms that do receive accreditation. Law firms can then share their scores and accreditation status with current clients and new prospects. The program is funded by law firms through an annual subscription fee; the results will be free to ACC members.

ACC has engaged a series of working groups with input from different industries to ensure the program effectively drives the safeguarding of sensitive legal information. An industry group of large and small firms, along with respected security experts, has been developing the initial "Core Module." The module pulls together relevant standards and controls from global security standards that are relevant to the security and management of legal data. The working group and the vetting process were created to ensure fairness and consistency throughout the program. Likewise, the In-house Advisory Board of ACC members has been reviewing program frameworks and elements to ensure they will meet the needs of in-house counsel. The accreditation program was reviewed for program elements, cost and risk to law firms, and compliance with ACC in-house requirements.

"Our firm, like many others, welcomes ACC's Data Steward Program," said John Kuttler, CIO at Finnegan, Henderson, Farabow, Garrett & Dunner, LLP. "Now we can do a detailed assessment once, and potentially

Unlike data security standards for financial services, for example, the legal profession does not have a basic set of rules for information security and information governance.

Firms that earn ACC accreditation will be authorized to publish this achievement, which will also be highlighted on *ACC.com* and communicated to ACC members.

leverage that assessment many times over with multiple clients. We particularly like that the program focuses specifically on the security and governance of client legal information. This guides us in ensuring that we are maintaining the appropriate level of security."

Detailing the Data Steward Program

The Data Steward program is designed to fit a variety of firms, from small, local firms with a handful of attorneys all the way up to the largest global firms. Key program elements include:

ACC Data Steward Program modules

At launch, the program includes core modules for each firm to assess, score, and securely share its information security status with selected clients. Some law firms have broader requirements, based on their practice specialties (e.g., healthcare, consumer marketing, financial services). ACC is prepared to offer additional modules based upon market interest, including a potential second module for advanced security requirements as well as industry and regional-specific modules such as GDPR and CCPA.

Self-assessment

A law firm that participates in the Data Steward Program begins by assessing its own performance against an industry-specific module of information security and governance controls. More than 40 controls have been specifically chosen for their relevance to the legal process. The core module also addresses security requirements for remote working. The self-assessment enables each law firm to test its current process against industry standards, both for benchmarking and sharing with clients. It also informs internal decisions about possible incremental security investments.

Scoring and benchmarking

As the law firm completes its self-assessment, the Data Steward Program will automatically review the assessment input and provide the firm with an objective score that compares its data security status to the framework's "perfect score." Scoring is based on a combination of core criteria that each firm must possess, combined with a set of flexible requirements that vary by matter, practice, size, and jurisdiction. It will also provide feedback on the firm's score relative to other firms in the industry. Firms participating in the Data Steward Program can leverage the results of their assessment by sharing the information directly from the system with the specific individuals at the clients or prospective clients it selects. Assessment and score data can be shared at granular levels.

Third-party assessment and accreditation

Independent validation of a law firm's information security capability is available in a second option from the Data Steward Program. A law firm that participates will engage an independent third-party assessor, accredited by ACC, to review and validate its results. This remote validation process includes a review of the entire assessment combined with an audit of randomly selected evidence. Successful completion will result in the firm being accredited by ACC. Firms that earn ACC accreditation will be authorized to publish this achievement, which will also be highlighted on *ACC.com* and communicated to ACC members.

Ongoing program updates

After initial release, program modules will be regularly updated to address new and emerging security threats. As the underlying security standards change, so too will the modules.

Why the Data Steward Program?

The Data Steward Program fits a clear, unmet need by both in-house counsel and law firms. The program provides a number of benefits:

- *Based on the best information security frameworks:* The controls were selected from the best information security frameworks

ACC EXTRAS ON... Protecting sensitive information

ACC Docket

What Your Business Needs to Know about the EU Cybersecurity Certification Framework (Feb. 2020). *accdocket.com/articles/eu-cybersecurity-certification-framework.cfm*

Everybody's Job, Nobody's Job: The Best Way to Create an Information Governance Program Without Going Crazy (April 2019). *accdocket.com/articles/resource.cfm?show=1500001*

The Next Step in Cyber Risk Readiness (Sept. 2019). *accdocket.com/articles/resource.cfm?show=1504705*

ACC HAS MORE MATERIAL ON THIS SUBJECT ON OUR WEBSITE. VISIT *WWW.ACC.COM*, WHERE YOU CAN BROWSE OUR RESOURCES BY PRACTICE AREA OR SEARCH BY KEYWORD.

in the market (e.g., NIST, and other global standards)

- *Specific to the legal industry:* The framework's controls have been specifically selected and optimized for their use and application in a legal services environment. The questions in the assessment are relevant.
- *Open, industry-based standards:* This guarantees that all industry participants "come to the middle" on context sensitive standards, benchmarking, and continuous improvement. This process can extend to embrace similar initiatives underway by other industry groups.
- *A level playing field:* The Data Steward Program has been built using an open, standard-setting process, resulting in context-sensitive standards and benchmarks that enable each firm to be compared consistently to its competitors.
- *Results build trust:* The program's scoring methodology — which includes a score for core information security capabilities, and combines it with validation information — to makes the results trustworthy to both client and law firms. The program will give ACC members and participating law firms a mechanism to drive better conversations as well as a tighter working relationship that ensures client data security.
- *Efficient:* The cloud-based assessment framework expedites the assessment process, collecting structured and accurate information about data security risks, while saving time, cost, and effort. It's easier and less costly to complete than a general information security framework (or hundreds of individual questionnaires).
- *Answer once, share often:* Law firms can complete the assessment once and share with new and prospective clients. This may alleviate or even avoid the need to answer a unique client questionnaire.
- *Proactive:* The framework and scoring system — specifically designed for law firms — enables the transition from simply collecting and organizing data about data security practices to prioritizing security investments.
- *Dynamic:* Firms can update their profile at any time and as many times as they wish. As they can add to their information security posture, their score is automatically updated, and you can easily inform your clients.
- *Defensible:* Compliance with industry standards offers ACC members, law firms, and legal service providers defensible due diligence.

ACC Leadership information security

The ACC Data Steward Program lays a path for one sector of the legal profession to use a single, common information security and information governance model. ACC's program eliminates the cybersecurity guessing game for ACC members and the law firms with whom they work. The ACC Data Steward Program can demonstrate to the rest of the legal community the importance of implementing one common approach to data security. Perhaps more importantly, ACC is taking an industry-wide, collaborative approach to raise information security and governance across the entire legal industry.

ACC is conducting a charter program to evaluate the program's procedures. The first charter occurred in the summer of 2020 with more than 10 firms participating. The second expanded charter program starts this fall with more than 25 firms participating in the evaluation. ACC's goal is to release the Data Steward Program sometime in early 2021. Information about the Data Steward Program for both in-house counsel and legal services providers is available at *www.accdatasteward.com*. **ACC**

NOTE

1 *www.wsj.com/articles/hackers-trigger-far-reaching-disruption-by-targeting-low-profile-firm-11592481600?emailToken=b9521773851ceb58be20058664897c64Rfes7PSGhGhZ5B5LOOW6dROp0rvj7dFMm7cQGC+Vioq0HESk1FFwyNhjZA6EEnnjR4RpvuaWA1npWsXQyHVCNKfEqlTfsLXEVa+ey837HjGqLFIOB7FoNrPhVQpmIzdGo7RInrV8Do+Uj+WDUcrZhg%3D%3D&reflink=article_email_share.*