



Portfolio Media, Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

ACC Launches Data Security Program For Law Firms

By **James Boyle**

Law360 (December 10, 2020, 1:58 PM EST) -- A new cybersecurity evaluation and accreditation program aims to provide an extra level of comfort for law firms looking to ensure their clients' data is protected.

The Association of Corporate Counsel announced Tuesday that it has officially launched its Data Steward Program, a cybersecurity assessment program targeted at law firms and clients in corporate law departments. In development since last year, the DSP will evaluate the software and policies law firms use to protect confidential client information and score their efficacy. Participating firms can also schedule an audit of their cybersecurity processes and receive an accreditation.

"All law firms, especially those working with in-house legal departments as clients, have data and cybersecurity at the top of the list of things that keep them awake at night," said Michele Shuster, founding partner of MacMurray & Shuster in New Albany, Ohio. "What ACC is doing is critically important, and they are drawing attention to the importance of data security for law firms."

MacMurray & Shuster started working with ACC's development team in January, Shuster told Law360, giving them tips and insight on how to serve small and mid-sized firms. The firm later became one of the first to pilot the program.

DSP is a two-tiered program, giving subscribing firms a choice for the system evaluation, according to the ACC's announcement. Tier 1 is a self-assessment conducted by the firm, where information on security software, policies and procedures are put into a program developed by Contoural Inc., an information governance consulting company.

The evaluation develops a score that firms can use to demonstrate to clients the efficacy of their data protection systems. Firms can also choose to use DSP's second tier, a custom, independent audit of the assessment score that could result in an accreditation, the ACC said. Shuster said in a phone interview that her firm is currently completing the first tier and will schedule an audit in the early new year.

"It's not about just measuring our antivirus software and technology," Shuster said. "We are also evaluating the procedures we use to protect information, like password security and two-factor verification."

The ACC said its creation of the DSP was prompted primarily by responses by the organization's members to surveys highlighting data security as one of their top issues. The platform was developed through an eight-person working group with backgrounds in legal services, information technology and information security.

"The ACC Data Steward Program provides both standardized, easily comparable evaluation, and, if desired, accreditation of law firms' security practices," Jim Merklinger, president of the ACC Credentialing Institute, said in a prepared statement. "It is a clear win-win for law firms and their clients."

The possibility of accessing sensitive client information has long made law firms a juicy target for cyberattacks. Shuster said it's a reality firms have been dealing with for more than 15 years as they have moved into the digital space.

"This is not an issue everybody is thinking about for the first time," Shuster said. "Security has been addressed for quite some time, developing software and honing procedures. ACC is providing a compliance benchmark that can be measured against other firms."

Two incidents in October brought the ever-underlying issue to the forefront. A **ransomware attack** at Seyforth Shaw LLP forced the firm to temporarily shut down its systems. The firm is working with the FBI to identify the hackers that blocked access to the company's data and demanded payment to restore it.

Later that month, Fragomen Del Ray Bernsen & Loewy LLP filed a notice with the California attorney general's office that an unauthorized third party **gained access** to personal information of some Google employees. The New York firm provides employment verification services for the company.

Experts **have described** incidents like these to Law360 as the "tip of the iceberg."

Michael Gold, a partner and co-chair of the cybersecurity and privacy group at Jeffer Mangels Butler & Mitchell LLP, told Law360 last month, "The frequency and magnitude of ransomware attacks are increasing. The hackers are getting way more sophisticated at executing these attacks, and this situation is not going to get better anytime too soon, unfortunately."

--Additional reporting by Xiumei Dong. Editing by Alyssa Miller.

All Content © 2003-2020, Portfolio Media, Inc.