Bloomberg Law

The United States Law Week

INSIGHT: Legal Industry Should Take Lead on E-Discovery Security Standards

By AJ Shankar

Posted March 5, 2019, 3:01 AM

Security of a client's sensitive information is doubly important during discovery when it's passed between opposing parties. Founder and CEO of Everlaw, AJ Shankar, calls on the legal profession to take the lead in improving security and calls for a unified set of tiered security standards.

Data security is important, but doubly so in litigation: often what's at stake isn't just any old data, but instead a client's most sensitive information, and it's typically passed between opposing parties without a comprehensive understanding of how it's going to be secured.

I propose creating a unified set of tiered security standards, from which parties can agree on a single tier based on the circumstances, to better facilitate meeting the responsibility to secure client data established in Rule 1.6 of the ABA's Model Rules of Professional Conduct.

Securing sensitive data isn't easy. It isn't as simple as using encryption or ensuring that your vendor's hardware provider has a particular certification. It is a holistic process, covering everyone who can access the data, from technicians to document reviewers to vendor support staff to law firm partners. Attacks are as likely to come through exploitation of human vulnerabilities, such as phishing, as they are through technical means.

Thus, when a sophisticated client, sometimes in conjunction with a law firm, selects a data vendor for litigation, great care is taken to make sure that the vendor meets stringent security and privacy requirements. Its entire security posture may be evaluated, including third-party certifications, penetration tests, audit histories, employee trainings, and business processes. As described by ABA Ethics Committee Formal Opinion 477R, the law firm itself should have its own controls, which may be similarly vetted.

Discovery: Hoping Both Parties Take Security Seriously

But in litigation, the story doesn't end there.

A key component in litigation is the production of relevant evidence during discovery. A client's sensitive data, often stripped of security guarantees beyond a temporary password, is handed over to opposing counsel, which, absent specific orders, may follow few security practices (or none at all) and can choose whichever vendor it wants. The producing party can only hope that the receiving party takes security as seriously as it does, even when the data does not belong to that party's clients.

To ameliorate this risk today, security requirements are typically conveyed in a protective order. Unfortunately, this case-by-case approach yields tremendous fragmentation: custom controls for each litigation, error-prone and hard to validate. For that reason, protective orders tend to be shallow, covering only easy-to-satisfy aspects of good security posture, rather than the holistic view that strong security demands—but that would typically make implementation and vendor vetting infeasible in the allotted timeframe.

Also, because these controls are one-off, it's easy to make mistakes. With a production protocol, the implications of a mistake are rarely devastating, but errors in a security protocol might well be. No one wants to make the kind of breach notification obligated by Formal Opinion 483 due to an inadvertent oversight in a protective order.

It's important for all parties to get security right. The industry stands to lose credibility with each high-profile data breach. Ignoring security places us further outside the normal constraints of business, rather than where litigation deserves to be in a country that operates under the rule of law: as an integral component of business operations and dispute resolution.

Conversely, being proactive about security furthers the role of lawyer as trusted advisor, positioning the practice of law not as an anachronism, but as forward-thinking, vibrant, and designed for the modern business environment.

At the same time, it's also important to recognize that security standards need not be completely uniform; as with the rest of litigation, proportionality matters. The security standards should suit the circumstances and the nature of the data being exchanged.

Proposed Solution: Tiers of Increasing Security

So I'd like to propose a robust solution that balances the need for security with the practical concerns around adoption and implementation. Doing so requires practitioners to value the long-term trajectory of the industry over the short-term benefits they may extract from the lack of standards on any particular litigation.

The industry model, in which law firms manage many litigations at once and are incentivized to take a broader approach than any one litigation might afford, allows for such a long-term view, and presents the opportunity to solve the security problem in a durable way.

My proposal is to establish a framework of tiers of increasing security. During litigation, the parties would simply agree on *which* tier to adhere to. Law firms and vendors could advertise the tiers they support, and on any particular matter each firm would only use vendors that were already certified for the agreed-upon tier.

What do these tiers look like? A simple formulation might be:

- Tier 0: minimum security: no standards other than secure transmission of production
- Tier 1: basic security: data is encrypted in transit and at rest; all access requires multi-factor authentication; data hoster (whether a vendor or on-premises) undertakes Formal Opinion 477R's "reasonable measures" for data security
- Tier 2: strong security: all parties have SOC 2 Type II in Privacy, Security, and Confidentiality
- Tier 3: advanced security: NIST 800-53 Moderate-Impact (federal standards)

In practice, these tiers could incorporate industry standards and questions from the EDRM Security Audit Questionnaire; determine agreed-upon weights, thresholds, and must-haves for each of the tiers, established by a working group of experts from across the industry, including folks from corporations, law firms, and vendors; be vetted by technical security experts, potentially from academia; and be regularly updated as security standards evolve.

Once established, individual tiers could easily be referenced and stipulated as part of a protective order: "The Parties shall adhere to the Ediscovery Security Reference Model v1.1, Tier 2 security standards."

Benefits and Risk Mitigation Outweigh the Costs

The adoption of this model is likely to increase proactive security costs for some legal organizations—potentially impacting access to justice—but the fallout from a breach due to bad security can far outweigh the costs of having good security.

More importantly, many good security practices, such as encryption, logging, and multi-factor authentication, do not demand extensive, ongoing costs. The quicker they are deemed essential, the quicker legal services organizations will adopt them as table stakes for which no premium is demanded. Ultimately, everyone will benefit from these improved security practices.

Adopting this model could be voluntary at first, and would be based on all parties recognizing the mid-term reciprocal value, and the ultimate long-term benefits to the industry, of adoption. In time, Judges may begin mandating adherence to certain tiers in Protective Orders, replacing the inefficient case-by-case approach with predictable security standards, freeing up judicial resources to focus on the next pressing matter.

Law has long suffered under the pejorative stereotype of legal practitioners as Luddites. In reality, our industry deals with some of the most complex and challenging technical problems around. I'd love to see us all take the lead in security as well.

Author Information

AJ Shankar is the founder and CEO of Everlaw. He has a Computer Science degree from the University of California, Berkeley and an Applied Mathematics degree from Harvard University. If you have feedback or interest in this project, you can reach Shankar at securitystandards@everlaw.com.