CORPORATE COUNSEL

3 Ways Cybersecurity Demands Are Changing E-Discovery

Data security responsibilities are changing discussions in pre-trial conferences and making e-discovery practitioners more cautious with data custodians.

Rhys Dipshan, Law Technology News

April 26, 2017

In a world where the pace of innovation often outflanks the law, e-discovery offers a bright spot. The policies and procedures that define e-discovery have, for the most part, kept pace with the changing demands placed on practitioners through new review technology and increasing data complexity. In addition to the 2015 amendments to the Federal Rules of Civil Procedure (FRCP), for example, the Sedona Conference also recently released its third edition of e-discovery principles.

While it may seem that cybersecurity guidance has been missing from e-discovery, the industry has lately become more aware of its cybersecurity needs , spurred in no small part by legal and the corporate sector's awareness of its own vulnerabilities. In Ernst & Young's "Cybersecurity in eDiscovery" webinar, experts discussed how this new e-discovery landscape is forming and what is driving its evolution.

Here are three highlights from the conversation on how cybersecurity is changing the world of e-discovery:

1. Data security is an increasingly pivotal part of pretrial conferences.

The 2015 amendment to FRCP Rule 26 requires opposing parties to hold pretrial conferences over their discovery requests and plans. Many of these discussions focus "on scope and setting—how [discovery will] be performed, and what will you get," said Todd Marlin, principal in Ernst & Young's forensic technology and discovery services practice. And for the most past, "data security is an afterthought."

In the midst of growing cyber threats, however, attorneys are fast realizing their obligation to delve into how opposing counsel and others intend to secure the discoverable data they obtain.

"The reality is that it has been an afterthought. As attorneys, it can't be going forward," said Kara Ricupero, director of e-discovery and records and information management at eBay Inc. Under the American Bar Association Model Rules of Professional Conduct, attorneys are obligated to competently protect their client's confidential information. These rules have been interpreted by many state bar associations to mean "if you don't know how to protect it, you bring someone in to protect it," Ricupero said.

Attorneys therefore will likely not be the only ones at the table in pretrial discovery conferences. Marlin expects information security professionals to become more active in negotiations.

In Ricupero's experience, such technical experts have been a vital resource for her when handling e-discovery demands. "It's so worth going out to lunch with your IT folks; the collaboration is needed."

2. There's more emphasis on best practices for data handling.

While it's important to scrutinize opposing parties' security policies, much of the inherent risk in transferring sensitive data can be mitigated before the information is ever handed over for discovery.

One vital way to accomplish this, Ricupero noted, is by having robust "information management [procedures] in-house," such as defensible disposal policies. Corporations and law firms that hold on to all the data they create and obtain will inevitably increase their security risk given that they "have that much more data to hand over."

Implementing defensible disposal practices is already underway in many law firms and organizations, given not only updated proportionality obligations under FRCP Rule 26(b), but upcoming compliance demands such as those put forth by the European Union's General Data Protection Regulation (GDPR).

Compliance and cybersecurity responsibilities have also pushed many corporations and law firms to implement "chain-of-custody" procedures that allow them to track sensitive data along its life cycle. Justin Hectus, chief information officer and chief information security officer at Keesal, Young & Logan (KYL), noted that "an effective security program has visibility to all your endpoints internally, and the same is true for when your data flows outside your organization."

Before relying on such procedures though, Marlin said corporations and law firms will likely first try to limit their sensitive information's exposure by not only redacting personally identifiable information (PII) in discoverable documents, but "taking the position that PII should not be produced in the first place."

3. Parties are looking for reassurances from every data custodian.

While limiting access to sensitive data is one of the most effective ways to prevent disclosures, it is not always possible in e-discovery. So corporations and law firms are increasingly looking to the next best step: getting reassurances that data is properly erased or secured when handled by other parties.

Ricupero, for example, noted she regularly requests her company's outside counsel to "reach out to opposing counsel to get them to return information, or destroy it and provide a certificate of destruction."

Data that cannot be erased or returned, however, is another story. As corporate counsel often need to rely on outside counsel and third-party vendors for e-discovery responsibilities, they are inevitable partners in the process.

This situation makes security audits of third parties "an absolute necessity," Ricupero said, and audits are becoming a standard requirement for those working with corporate legal departments. "I definitely think that's one of the things we are requiring more and more when I talk to other people in the same space who are in similar-sized companies."

While Ricupero noted that vendors are open to such audits: "When it comes to law firms, I see little more pushback there." But she added that many are fast realizing that security assurances are a business necessity and significant differentiator in the law firm market.

Hectus, for example, noted that his law firm regularly "undergoes around 20 such [security] audits every year—and they range from a 20-point questionnaire to a three-day on-site visit."

Contact Rhys Dipshan at rdipshan@alm.com. On Twitter: @R_Dipshan.
