How to Mitigate Risk When Handing Data to Outside Law Firms

November 17, 2015

RELATED CONTENT

Ever since the cybersecurity firm Mandiant reported in 2013 that 80 percent of the country's largest law firms have been hacked, numerous surveys have shown that **client pressure (http://insidelegal.typepad.com/files/2015/08/2015_ILTA_InsideLegal_Technology_Purchasing_Survey.pdf)** is causing the largest firms to **spend millions** (http://ccmchase.com/cybersecurity-report-download/)encrypting communications, protecting mobile devices and beefing up security.

But what happens during eDiscovery, when a client's most sensitive information must be disclosed by court order to another law firm, which may or may not be as vigilant about cybersecurity?

"eDiscovery is [really] fraught with a fair amount of risk," said Aaron Crews, senior associate general counsel and head of eDiscovery at Walmart.

Crews explained: Normally, a company stores all of its data, including its most sensitive items among vast troves.

"The gems of your data, the really risk-bearing stuff is kind of hidden among the rest of the data," he said. "But in the eDiscovery space, you're hosting a slice of data that has been particularly selected because it has those gems in it."

During eDiscovery, that sensitive data could be turned over to a law firm that lacks adequate cybersecurity.

To protect against a data breach in the context of discovery, some practitioners have begun requiring their litigation adversaries to sign protective orders. Crews said he asks the opposing side to agree to one of the following three provisions:

1. To sign a protective order attesting that their firm meets certain basic cybersecurity protocols and that it indemnifies his company against any risk of breach.
2. To use a trusted eDiscovery vendor.
3. If all else fails, it must access the data through his own trusted eDiscovery vendor.

Paul Weiner, a shareholder at Littler Mendelson who is national eDiscovery counsel for the firm, said he drafted an order with such protections because the risk and consequences of a data breach during eDiscovery are simply too great to ignore.

He noted that the protective order requires a judge's approval, adding that so far he hasn't experienced any problems or push back.

Below is a sample of the language that Weiner is using in the protective orders that he asks litigants to sign before a discovery production:

> **Information Security Protections**
> Any person in possession of another party's Confidential Information shall maintain a written information security program that includes reasonable administrative, technical, and physical safeguards designed to protect the security and confidentiality of such Confidential Information, protect against any reasonably anticipated threats or hazards to the security of such Confidential Information, and protect against unauthorized access to or use of such Confidential Information. To the extent a person or party does not have an information security program they may comply with this provision by having the Confidential Information managed by and/or stored with eDiscovery vendors or claims administrators that maintain such an information security program.
>
> If the Receiving Party discovers a breach of security, including any actual or suspected unauthorized access, relating to another party's Confidential Information, the Receiving Party shall: (1) promptly provide written notice to Designating Party of such breach; (2) investigate and take reasonable efforts to remediate the effects of the breach, and provide Designating Party with assurances reasonably satisfactory to Designating Party that such breach shall not recur; and (3) provide sufficient information about the breach that the Designating Party can reasonably ascertain the size and scope of the breach. If required by any judicial or governmental request, requirement or order to disclose such information, the Receiving Party shall take all reasonable steps to give the Designating Party sufficient prior notice in order to contest such request, requirement or order through legal means. The Receiving Party agrees to cooperate with the Designating Party or law enforcement in investigating any such security incident. In any event, the Receiving Party shall promptly take all necessary and appropriate corrective action to terminate the unauthorized access.