GT GreenbergTraurig

Why Cybersecurity Matters in High-Stakes Litigation

Preserve, preserve, preserve … but what about protect?

By Avi Benayoun and Chelsea Koff | April 13, 2018 | New Jersey Law Journal

You're a skilled general counsel embroiled in high stakes litigation, perhaps even a "bet the company" case. You've dotted your i's and crossed your t's, all in preparation for the ensuing battle. You've issued appropriate litigation hold letters, you've backed-up case-critical electronically stored information (ESI), you've taken steps to ensure that potentially relevant ESI is preserved, and that nothing is modified, deleted or "rolls off the system" without you knowing about it first. You go to sleep believing that you've taken all reasonable steps to preserve the data that may one day be necessary for your lawsuit.

The next morning you wake up to an email from your IT department stating that a data breach has occurred, that the company is investigating the extent of the breach, and that more details will follow. You first think about your own files, hoping that nothing has been lost; but then your attention inevitably shifts to the lawsuit and all the data that you worked hard to preserve: What if any of the data has been compromised or, worse yet, lost? Can the company be blamed for a failure to preserve? Could this actually cause us to *lose* the case?

Whether used for marketing, analytics or research—or for other more nefarious purposes—data is the modern-day gold, and we're in the midst of a gold rush. As technology evolves at an ever-faster pace—and data becomes increasingly valuable—ransomware and cyberattacks will continue to be on the rise. This article addresses some of the potential impacts of a data breach on pending litigation, and whether cybersecurity checks should become just as much a part of a company's data preservation plan as the now-routine litigation hold letters.

Data is Gold

Data is the gold that drives many high stakes litigation matters. When a party reasonably believes that future litigation is foreseeable, its "duty to preserve" is triggered. *David's Bridal v. House of Brides*, 2009 WL 10690590, *2 (D. N.J. 2009) (citing *Kronisch v. United States,* 150 F.3d 112, 126 (2d Cir.1998)) (the duty to preserve arises "when a party should have known that the evidence may be relevant to future litigation."). "While a litigant is under no duty to keep or retain every document in its possession, even in advance of litigation, it is under a duty to preserve what it knows, or reasonably should know, will likely be requested in reasonably foreseeable litigation." Scott v. IBM Corp., 196 F.R.D. 233, 249 (D. N.J. 2000). But what exactly does the duty to "preserve" entail?

We know that at a minimum the duty to preserve includes: (i) notifying custodians of potentially relevant ESI regarding their preservation obligations; (ii) stopping the routine purging of potentially relevant ESI; and (iii) suspending document retention/destruction policies that could compromise potentially relevant ESI. *State Nat'l Ins. Co. v. County of Camden*, 2011 WL 13257149, *3 (D. N.J. 2011) (collecting cases). Because potentially relevant ESI is not necessarily collected when the duty to preserve is triggered, a party's handling of the non-collected ESI can become important. While the ESI that has been collected—whether imaged and backed up or collected by an eDiscovery vendor—should be deemed to be safe if handled correctly, it is the ESI that is not collected but rather "preserved" by the litigant itself that keeps some litigators up at night because its handling can impact the course of any litigation.

The Duty to Preserve is not Boundless, but it Does Include a Duty to 'Safeguard'

"The scope of the duty to preserve data is not boundless. A party 'need do only what is reasonable under the circumstances.'" *Van De Wiele v. Acme Supermarkets*, 2015 WL 4508376 *3 (D. N.J. 2015). The recently amended Rule 37(e) recognizes that "reasonable steps" to preserve suffice; it does not call for "perfection." Fed. R. Civ. P. 37(e) Advisory Committee's notes to 2015 amendment. And, what is "reasonable" is a fact question to be determined on a case-by-case basis. *Friedman v. Philadelphia Parking Authority*, 2016 WL 6247470 *7 (E.D. Pa. 2016).

Likewise, not all parties are created equal when it comes to evaluating their preservation efforts. Case law and authorities teach us that courts should be sensitive to factors such as a party's sophistication and financial resources in determining whether that party acted "reasonably." *Friedman*, at *7; Fed. R. Civ. P. 37(e) Advisory Committee's notes to 2015 amendment. So when it comes to cybersecurity measures, a sophisticated, global company accustomed to regularly handling confidential information may be held to a different standard than a small local company that never touches sensitive data.

In the past, litigants often preserved their data via "backup drives"—physical tapes or external hard drives stored in locked fireproof rooms or off-site at storage facilities safely protected and away from thieves and hackers. Now, the term "backup drive" more often than not refers to a live database such as a cloud based or other live storage medium. Why does this matter? Because, as the seminal case of *Zubulake* taught us, the failure to "safeguard" backup tapes can result in sanctions for spoliation of evidence. *Zubulake v. UBS Warburg*, 229 F.R.D. 422, 424 (S.D.N.Y. 2004).

This begs the question—should a litigant ask how its data is not just being "preserved" but how is it being "safeguarded"? If a litigant stores its physical "backup drive" in an unlocked common area desk drawer where thefts have been known to occur rather than under lock and key, that litigant may not find much sympathy from the court when it explains that the backup drive was stolen. The same could be said for data stored in the cloud with no security measures in place after repeated cyberattacks. In the end, data

that is either unsecured or under-secured could be open season to anyone from a common thief to a sophisticated hacker looking to strike gold.

Cyberattack: A Superseding Cause?

The duty to preserve is flexible. A litigant is not the absolute guarantor of the safety of its data, and will not be held culpable when the loss of information occurs "by events outside the party's control," including through a "malign software attack." FRCP 37, Adv. Comm. Notes. That is because Rule 37(e) "is inapplicable when the loss of information occurs despite the party's reasonable steps to preserve." *Id.* *"Courts, however, may … assess the extent to which a party knew of and protected against such risks."* *Id.* (Emphasis added.) So, as contemplated by the Committee Notes to Rule 37(e), foreseeability of a cyberattack should at least be considered when it comes to a party's preservation efforts because a company may not be immune from liability where its data is lost due to some intervening causation, including an intentional cyberattack by a third party.

Although New Jersey courts have not directly addressed a party's preservation efforts in the context of a cyberattack, they have followed tort law when determining if a superseding act may break the chain of causation that links the alleged wrongful act—here, a litigant's failure to preserve potentially relevant ESI—and the injury suffered. As explained in *Komlodi v. Picciano*, 89 A.3d 1234, 1252 (N.J. Super. 2014), intervening causes that are foreseeable or the normal incidents of the risk created, will not break the chain of causation and relieve a party of liability. *Id. citing* Model Jury Charge (Civil) 6.14 (Aug. 1999). Thus, the concepts of foreseeability and superseding/intervening causation are inextricably interrelated and the court needs to have a full understanding of both. *Komlodi*, at 1252. Under this framework, if we assumed a litigant has had a history of attempted cyberattacks and nevertheless stored potentially relevant ESI in the cloud with limited or no security measures in place, a court may find that any ensuing data loss caused by a third-party attack was foreseeable and, therefore, the intervening cause may not excuse its failure to preserve.

Should Litigators Consider a 'Cybersecurity Check'?

The need for a "cybersecurity check" is not one-size-fits-all and will likely depend on a number of factors including: (1) the nature of the litigant itself and its business; (2) whether the litigant implemented standard cybersecurity measures expected to be in place in its industry; (3) whether cyberattacks are foreseeable or have occurred in the past; and (4) the extent to which the litigant has protected against the reasonably foreseeable risks. The answer as to whether a "cybersecurity check" is needed, boils down to whether a court could consider an unprotected or under-protected data breach a failure to "safeguard" sufficient to warrant the imposition of sanctions after applying these factors.

In the months and years to come, lawyers, litigants and courts will be forced to grapple with third-party attacks on electronic data and will eventually expand on a litigant's duty to "safeguard" potentially relevant ESI. Will the duty to preserve include or even require a "cybersecurity check," and will the failure to include one expose a litigant for failing to meet its duty? For now, adding that extra question to counsel's general preservation protocols—how is the data protected?—could help militate against that risk.

About the Authors:

Avi Benayoun is a shareholder with Greenberg Traurig, focusing his practice on complex commercial litigation. Chelsea Koff is an associate in the firm's Litigation Practice. They are resident in the firm's Fort Lauderdale office.

Avi Benayoun
benayouna@gtlaw.com

Chelsea Koff
koffc@gtlaw.com