Sponsored by EY Forensic & Integrity Services

Cybersecurity in eDiscovery

Of special interest to:

General counsel
Outside counsel
Chief legal officer
Legal technology executives
Chief technology officer
Chief compliance officer
Chief information security officer

Legal, Compliance and Technology Executive Series

Keywords. Deposition schedules. Clawback agreements. These terms are engrained in the vernacular of the litigation warrior and are issues often hotly contested as part of the pre-trial meet and confer. Yet addressing the issue of cybersecurity continues to challenge many attorneys as they prepare for these negotiations, despite the front page headlines broadcasting the inherent danger.

The use of outside eDiscovery vendors to manage the eDiscovery process has become commonplace in today's evolving business landscape. But oftentimes organizations fail to properly validate that the software applications they use or their vendors use, whether off-the-shelf or custom, incorporate sufficient protections against a cyber breach. That is just one of many cybersecurity challenges that increasingly affect today's eDiscovery efforts. There are also many perils within an organization's own eDiscovery process that need to be managed before potential disaster strikes.

EY
Building a better working world

Litigating in the age of attacks

The *National Law Review,* January 2017 edition, labeled 2016 as "the year that law firm data breaches landed and stayed squarely in both the national and international headlines."[1] Numerous infiltrations targeting law firms and client data affirmed the FBI cyber division's alert of March 4, 2016, warning large firms that "hackers were targeting them."[2] Multiple publications, including *The Wall Street Journal* and *Fortune* magazine, reported that law firms were the subject of cyber attacks in early 2016 due in large part to their roles as legal counsel to many of the top global financial institutions.

In April of 2016, the Panama Papers rocked the legal and business worlds when hackers breached the law firm Mossack Fonseca in Panama, resulting in the disclosure of millions of documents related to business operations of hundreds of companies and high-profile individuals.

[1] Kathryn T. Allen, "Law Firm Data Breaches: Big Law, Big Data, Big Problem," The *National Law Review,* January 11, 2017, http://www.natlawreview.com/article/law-firm-data-breaches-big-law-big-data-big-problem.

[2] Gabe Friedman, "FBI Alert Warns of Criminals Seeking Access to Law Firm Networks," *Bloomberg Law – Big Law Business,* March 11, 2016, https://bol.bna.com/fbi-alert-warns-of-criminals-seeking-access-to-law-firm-networks/.

Authors

Todd Marlin, Principal
Ernst & Young LLP
todd.marlin@ey.com

Piyush Dixit, Senior Manager
Ernst & Young LLP
piyush.dixit@ey.com

Shawn Fohs, Senior Manager
Ernst & Young LLP
shawn.fohs@ey.com

In light of the pronounced risks of exposure, companies and their counsel are wise to confirm that all the participants in the eDiscovery process – eDiscovery vendors for both parties, all counsel handling the data and even the in-house teams – have employed reasonable data security measures throughout the process. Lawyers acknowledge their legal obligation to protect their clients' confidential data not just by instituting policies in their own environment, but by requiring and validating that equal protections are being provided by anyone receiving the data during the discovery process. And the time to start that discussion is the meet and confer.

Cybersecurity at the Rule 26(f) pretrial conference

Imagine you're in the midst of discovery on behalf of your corporation or a corporate client entangled in a highly public intellectual property (IP) dispute. The data you are producing is sensitive and confidential. Now imagine if that sensitive data were infiltrated by a cyber attacker through your opposing party's production database. Your company would suffer the consequences of this breach. You might comfort yourself that since the cyber attack wasn't on your system it was out of your control. But what could you have done during the pre-trial conference to reduce the risk of this occurrence? And what responsibilities does your opposing counsel have to disclose and remediate the breach? Given the sensitive nature of data exchanged, should cybersecurity protocols, requirements and remedies be negotiated and agreed in advance?

Rule 26(f) of the Federal Rules of Civil Procedure requires that parties meet early in a litigation to cooperatively establish a discovery plan that outlines how the action will proceed and the scope of discovery. Traditionally, the meet and confer negotiations related to electronically stored information (ESI) focus on topics such as custodian lists, relevant data sources and discovery deadlines in order to establish discovery obligations and requirements. Yet, one topic that commonly gets overlooked in these negotiations is the obligation of each party, under relevant data protection laws or regulations, to employ reasonable security measures when handling information obtained in the discovery process. This is usually due to a lack of awareness of cyber breach protocols and the resulting liability for such an event.

However, the American Bar Association Model Rules of Professional Conduct, in an increasing number of states in the US, have added language that requires counsel to display technological competence. Specifically, it mandates understanding "the benefits and risks associated with relevant technology," as well as the skill to prevent the inadvertent disclosure of client data. Attorneys who omit any mention of data security during the meet and confer fall short of this standard. They do this at their own increasing peril, as the Panama Papers leak has shown. Firms and attorneys that suffer a data breach could face serious consequences such as regulatory investigation, internal investigation costs and civil lawsuits brought about by clients, customers and shareholders. The more common cyber breaches become, the more important it is to invest the energy from the start of discovery to protect the information exchanged, and to establish disclosure and remediation protocols that are binding on the parties in the event of a breach.

Counsel's considerations during the meet and confer

Data transfer between parties

Transferring data from one party to another, whether from a client to an eDiscovery vendor or between two law firms, is one of the most vulnerable areas when it comes to cyber breaches. For example, an organization responding to a discovery request may elect to collect data from local email servers, network shares and other

information sources and then send that data directly to counsel via standard email or physical media. When data is ready for processing, review or production, similar methods are often used to transfer data, which presents cyber criminals with significantly fewer obstacles to circumvent. As an alternative, parties may wish to establish explicit security measures in the Rule 26 discovery plan for the transfer of data, such as the use of standard secure file transfer applications when documents are exchanged among attorneys and where the data is automatically deleted after download. Consideration should also be given to data handling procedures that include network security protocols and monitoring of the network when data is being reviewed. Implementation of database credentials that require two-factor authentication and are refreshed on a periodic basis are simple defense measures to deter unauthorized data access. Additionally, use of redactions for propriety and highly sensitive segments of the data (personally identifiable information (PII), privilege, trade secrets, etc.), is another security measure that should be agreed to by both parties.

Due diligence on eDiscovery service and technology vendors

Both parties should also come prepared to discuss the safeguards and protections in place with the eDiscovery service vendors that will be involved from both sides. To address this, there should be a basic understanding of where their data is being held, which individuals have access to the data and the security measures in place at each vendor to limit unauthorized access. Information regarding the vendor's data protection and security program, as well as any issued security certifications or third-party audits, enable comparison to industry standards.

Looking past the service providers, the Rule 26 discovery plan should also establish a minimum set of standards for eDiscovery software tools used and how to vet them. Some critical software features to consider include dual-factor authentication, access permissions following a least privilege approach and network scanning method.

Duty to disclose security breaches and plan for post-breach mitigation and remediation

The parties should discuss what they consider to be a security breach and establish an appropriate amount of time to disclose the breach. State data breach notification requirements provide a baseline. The parties could agree that even if those notification thresholds are not met, they will still be obligated to notify one another in the event of a breach. Any agreed upon protocol for notification of a breach should include specific provisions on the type of information to disclose, as well as how quickly a party must notify other parties after a breach has been detected. Examples of the questions to guide breach notification include:

Has a non-intended party gained access to any of the produced information?

- Has the breached data been identified on the internet or dark web?
- Have any of the systems that share a network with produced data been breached?
- Have any employees or attorneys exceeded their level of access?
- When was the breach first discovered?
- Has the source of the breach or the method by which the breach took place been identified?
- What parties are currently aware of the unauthorized access?

Data disposition considerations

Both parties should agree to data disposition after a matter has finished, including timing and methods for data disposition. In situations, where the requesting party is a government or regulatory agency, counsel should seek clarification on the required retention period and the use of secure off-line locations for non-active data. The data disposition plan should account for all locations of the data, including data stored on servers by the attorneys who worked on the matter, data hosted by any third parties and data produced to the adversarial party. Examples of a baseline data disposition protocol should be able to answer the following questions:

- Are both electronic and physical data disposition methods agreed upon?
- What methods are being used to make sure data is disposed of from all network locations?
- What methods are used to determine all data was disposed of from attorney's computers and email?
- Is there confirmation from third parties that all data has been disposed of using an agreed-upon method?
- Is there an agreed-upon amount of time allowed to complete the data disposition?
- Who is responsible for certifying that the disposition was carried out in a reasonable manner?

Data security in your direct control

We've discussed at length the measures and steps that parties involved in a dispute that involves eDiscovery should consider as part of the meet and confer. However, to better prepare for cyber threats, organizations and their legal counsel should conduct periodic assessments of their own internal security practices to confirm that the safeguards in place are providing reasonable mitigation of the risk of data breach. Such assessments should include an annual assessment performed by a neutral party that can perform an independent review. When the review is satisfactory, the certified result will demonstrate to adversaries in a discovery matter that cybersecurity has been considered in the ordinary course of business and not as a by-product of a discovery request. eDiscovery presents significant challenges to handling data and safeguarding it from unauthorized disclosure. Litigation, investigations and similar matters typically involve highly sensitive data. A logical starting point to

data security for discovery is to establish a defined protocol that follows the discovery process flow and defines security controls at each phase.

For data collection and transfer from litigant to counsel or a vendor:

- Use of secure file transfer applications
- Use of Advanced Encryption Standard for data in transit and at rest
- Thorough documentation of chain of custody and evidence tracking

For processing, hosting, review and production:

- Use a segregated network
- Review the security controls of the tools used to see if they possess any security certification
- Review off-the-shelf or custom-built software for the use of secure coding principle
- Document the identity and access control measures used
- Define data access privilege based on segregation of duties
- Establish safeguards to prevent exports of data during processing or within the hosted environment
- Establish protocols to track exports of data from the hosted environment, as appropriate
- Disable the use of USB devices
- Obtain an independent assessment of the controls and security available using industry standards such as SOC II, SAS 70, etc.

Finally, collaboration between legal and information security teams is paramount. About half of the 51 general counsel surveyed for the 2017 General Counsel Report, published by the Consero Group, in partnership with Fisher Phillips, cited data privacy and cybersecurity risk as their top challenge. It is not surprising that the need for law department leaders to collaborate with their security teams is more important than ever. Create a task force composed of both legal and IT professionals, who are comfortable with technology and sensitive to the potential risks associated with its use.

Conclusion

With the increased targeting of lawyers and law firms, attorneys should make it their responsibility to understand the role they play in cybersecurity, and how to best mitigate cybersecurity risks on behalf of their clients. The risks of monetary, reputational and professional damage that are associated with a cyber breach are simply too great to ignore. Ultimately, a joint approach between legal and IT to data security can help an organization prevent, respond to and recover from a breach more comprehensively than if each operated in a siloed fashion. After making this internal investment in collaboration, legal teams should apply their knowledge of data security to their Rule 26(f) "meet and confer" sessions so that data security is no longer overlooked because of attention to more traditional areas of concern.

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

About EY Forensic & Integrity Services
Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority – no matter the size or industry sector. With approximately 4,500 forensic professionals around the world, we will assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide.

EYG 02554-181Gbl
1807-2805276

ED None

ey.com