

Special Feature

Plan for eDiscovery before, not after, crisis

By Cristina Lenares Antalik



The senior vice president of software development leaves your client's company and forms a competing company. Soon after the VP's departure, other employees join her at the new company.

Then your client notices that many of

the company's once-loyal customers have decided to "go with someone else." Upon further investigation, it turns out they've gone to the competing company. Your client suspects some trade secrets have also left with the ex-employees.

Your client wants justice and calls you.

As you begin to understand the case, you identify potential custodians who may have relevant electronically stored information, or ESI. You ask your client some simple questions about the departed custodians: Did the employees have company-issued computers or phones? Did they use personal devices or personal email accounts for work purposes? Where did they store data on the company's network? Did they use any external drives? Did they have access to cloud-based accounts or secure transfer programs?

Cristina Lenares Antalik is the electronic data discovery manager at Elysium Digital. She has extensive experience advising law firms, government agencies and corporate clients in the areas of data and case management strategy and best practices.

Suddenly these simple questions feel very complicated, and your client begins to panic. You need answers that your client may not be able to provide. Other employees at your client's company hear of the litigation and, fearing that their personal communications may be subject to preservation and collection, they delete personal emails from their work accounts — communications potentially critical to the case.

Your client was not prepared for litigation and has limited insight into where to find the information you need.

Unfortunately, this scenario is often the case for companies in an age of shifting loyalties and easily moveable data. Far too many companies facing litigation are not prepared to deal with requests for electronic evidence.

A company that has been involved in litigation or an investigation is more likely to follow your advice to prepare. Some clients, however, will argue that litigation readiness involves a lot of "overhead" for a situation that rarely (if ever) arises.

But the cost of being prepared is dwarfed by the potential losses due to lack of preparation. Litigation readiness is like automotive insurance: You hope that an accident will never happen, but when it does, you're glad that you have it.

When to prepare clients for eDiscovery? Right now

There are several relatively simple, yet critical, ways an attorney can help prepare a company in advance for litigation and avoid many of the pitfalls of being caught off-guard.

1. Develop and enforce a clear data storage and retention policy

Having a documented policy will remove ambiguity for employees regarding data reten-



tion and destruction, while clearly outlining good data storage procedures for employees to follow. Enforcement of the policy is critical. Employees should be trained on the mechanics, and testing should be conducted regularly to gauge compliance.

At a minimum, a company should consider the following when devising its data storage and retention policies:

- permissible data storage locations controlled by the company such as business computers, network drives, flash drives and mobile devices;
- permissible data storage locations allowed by the company including home computers, flash drives and personal mobile devices;
- industry laws and regulations governing the retention of data;
- auto-deletion policies such as time-based auto email purge;
- offline storage including backup tapes and offsite archiving services;

- defined roles and clear responsibilities for policy refresh and compliance enforcement.

2. Know where data is stored

Understanding and recording where employees save the company's electronic information is critical. It is important to have a readily accessible map of where data sources reside for ongoing data management. Having a data map enables a more rapid response to litigation or an investigation by helping efficiently identify data sources and prepare for custodian interviews.

Companies should consider the following when creating a data map:

- business units within the company, employees who work in each business unit, the physical location of each employee and the systems each employee uses;
- company-issued devices and personal devices approved for work use, including to whom they were issued as well as their makes, models and serial numbers;
- company-issued email accounts and personal email accounts approved for work use for each employee;
- employee access to software applications, databases, systems and shared network resources;
- cloud-based accounts used for work purposes including Dropbox accounts, SaaS environments and others.

3. Define and implement a legal hold plan

Legal hold is a process by which potentially relevant data is preserved in anticipation of litigation or an investigation. Having a pre-defined, documented, legal hold strategy can make legal hold a much more streamlined and manageable process for all involved.

An important step in creating this plan is to identify a legal hold response team. At a minimum, the team should include members from the company's legal, information technology and records management departments. Companies should consider including representatives from all groups who are needed to affect and ensure compliance with a legal hold.

A legal hold strategy should clearly define roles for each member of the response team, including responsibilities for identifying data

sources, suspending auto-purge policies, and communicating with data custodians regarding their preservation obligations. At the direction of counsel, this team is responsible for taking reasonable steps to avoid data spoliation.

What if my client is unprepared? Get to know their data

Imagine that you are representing the defendant in the scenario outlined at the beginning of this piece. Your client is the former senior VP of software development who started a competing company. Litigation has been filed against her and her new company. Your client was not expecting to be sued and is not prepared for litigation. What do you do?

There are several steps you can take to minimize the impact of being unprepared for eDiscovery. It is imperative that a legal hold be initiated and data preserved. Once the data has been preserved, the risk of spoliation significantly decreases.

After preservation, a company should take the time to assess its data and help you understand what it has in its possession. Knowledge is power, and knowing the potentially relevant data is a powerful negotiation tool.

Assessing the size and complexity of the data can give you a big advantage in negotiating with the opposing party. Servers typically contain large quantities of data, but if the custodians who are party to the litigation had access only to one small directory on the server, negotiating collection of only the one directory could save tens of thousands of dollars in ESI processing during eDiscovery.

If the involved custodians do have a significant amount of potentially relevant data, understanding the types of data may help justify the

Considerations when preparing for eDiscovery

- Assess the size and composition of the data to determine the need for outsourced collections, processing and hosting.
- Determine feasibility and value of employing technology such as near duplicate analysis or predictive coding.
- Plan your eDiscovery workflow including processing, deduplication strategy, keywords, date filters and size of review team, and align with known compliance deadlines.
- Evaluate production formats that best suit your needs and budget; options include native production, bates-stamped TIFF production and in-database production.
- Build a data management and oversight team, either internal or outsourced.

use of technologies such as computer-assisted review, thereby reducing the costs associated with traditional linear review.

Another benefit of knowing the data is identifying proportionality issues in a case. Calculating potential eDiscovery costs early in the process can uncover proportionality issues, meaning that the costs for eDiscovery are disproportionate to the claim at stake.

Waiting to assess data can put you and your client in a position to fail. The sooner you, as legal counsel, understand how much potentially relevant data there is and the type of data that exists, the sooner you can plan your negotiation strategy and plot the path to success.

Conclusion

No matter how you slice it, eDiscovery is complicated, and navigating its technical nuances is an arduous

process. Avoiding or delaying will not make it go away; it will only lead to difficult conversations with irate judges and unhappy clients.

Educate your client while you have the opportunity. Teach the client the steps: Build an internal process and team; hire qualified eDiscovery consultants, if necessary; and lay the foundation of litigation readiness.

Reasonable forethought and planning can reduce risk, save substantial cost, and position you and your client for future success. **MLW**

Elysium Digital is a technology litigation consulting firm with a 15-year history of helping clients address the toughest challenges at the intersection of law and technology. In addition to Elysium's eDiscovery services, the firm has a full-service digital forensics practice and an intellectual property practice which provides both consulting and expert testimony for technology-related legal matters.

Elysium Digital offers full digital forensic and eDiscovery services. For more information about our services, please contact us at: 617-986-3850.
www.elys.com



ELYSIUM[®]
DIGITAL

YOU KNOW THE LAW. WE KNOW TECHNOLOGY.[®]