“Just because something may be technically defensible doesn’t mean it is legally defensible.”

eDISCOVERY: PITFALLS AND HOW TO AVOID THEM

Many companies that regularly navigate the challenges of eDiscovery still suffer significant inefficiencies. There is, however, a way to eliminate many of these inefficiencies, while still achieving compliance.

In electronic discovery, as in most things, it’s best to learn from others’ mistakes. Consider one company’s decision to handle its own eDiscovery needs. Facing a class action lawsuit, the firm’s leaders determined, reasonably enough, that an estimated cost of $30,000 for data collection was a lot of money. They concluded further that they had capable, highly trained IT staff who could collect the necessary emails and other electronic files for the suit’s discovery phase. Nevertheless, their decision cost the company an additional $800,000 to answer a plaintiff’s claim of spoliation of evidence. They simply didn’t have the knowledge or tools to correctly gather and share data in a legally defensible way.

While larger companies are unlikely to take a comprehensively do-it-yourself approach to eDiscovery, they are prone to making similar mistakes — such as thinking in terms of “data” rather than “evidence,” and involving unqualified individuals in the chain of custody of that evidence collection and handling. Just because something may be technically defensible doesn’t mean it is legally defensible. And even in cases where companies partner with eDiscovery providers, they are likely to significantly overspend on the process through lack of standardized systems and processes.

EMERGING CHALLENGES OF eDISCOVERY

Getting eDiscovery right is rapidly increasing in importance for two reasons. First, business is increasingly global, and economic development is driving up the frequency of litigation in many geographical areas. Second, and more urgent, the creation and consumption of data by businesses is skyrocketing, leading to rapidly increasing amounts and types of data that can be relevant in legal actions. Few companies are keeping up with these changes in the way they should if they are to be prepared for potential legal challenges.

At one end of the spectrum are companies that have never experienced eDiscovery and simply don’t know where to start. Like the company in the above example, they take a seat-of-the-pants approach or recognize they don’t even know where to start and turn to partners. At the other end of the spectrum are companies that are reasonably savvy and experienced in eDiscovery, but tend to be inefficient because of multiple partners, fragmented processes and disparate systems.

FRAGMENTARY PROCESSES AND SYSTEMS

In many cases, companies leave management of eDiscovery partners to legal counsel. While that may provide competent oversight, it can lead to serious inefficiency. One reason is that law firms in different jurisdictions are likely to partner with different eDiscovery firms, which means losing potential advantages associated with a single eDiscovery partner — advantages such as preferred local service providers, preferred pricing and volume discounts. More important, law firms may act without deference to their client’s budgetary constraints. In such situations, where a partner may lose sight of a client’s financial best interest, a given case can become a black hole of expense, with legal counsel ordering services without regard to cost. Companies similarly often leverage multiple, redundant eDiscovery systems, or continue to run inefficient legacy systems of acquired entities.
In the case of both systems and partnerships, compliance is typically offered as the rationale for multiple, disconnected capabilities; and, where there are different jurisdictions, companies often believe it is prudent to maintain distinct capabilities. However, a single system and partner paradigm can actually support the goals of both compliance and efficiency through standardized, repeatable processes and workflows that leave room for jurisdictional differences.

Fragmentation of systems and processes also opens the door to irregular treatment of data, particularly for global companies whose data may reside in multiple jurisdictions. In the discovery process, data becomes evidence, and evidence requires a higher standard of care. Parties to a suit must be able to demonstrate an unbroken chain of custody of evidence, preserved in its original state, in a forensically sound manner. This requires the use of both proper tools designed to preserve the evidence’s metadata and an audit trail from beginning to end.

Too often data-collection tasks are assigned to IT professionals who are not forensically trained or certified. It is not unusual under such circumstances for data to be accidentally deleted, and there is a chance discovery will be either under- or overinclusive. Well-trained IT staff may properly encrypt data before sending to an eDiscovery partner, but at any time during transit it could be intercepted or compromised — or even simply sent to the wrong address. When the discovery process reaches across national borders, the risk is even greater.

In cases where a major regulator is involved — say, the U.S. Federal Trade Commission (FTC) — demands for evidence may simply be too great for staff, trained or not, who lack the proper tools and accelerators. In an acquisition review, for example, the FTC issued a 20-page production request and gave the company 90 days to fulfill it. The result was more than 12 million electronic documents, amounting to more than 30 terabytes of data. There is no way the FTC could review all of that evidence, but the company couldn’t take the risk that the regulator would randomly select something that could jeopardize the acquisition. For the company to identify pertinent documents to fulfill the request, it needed the proper strategy and capabilities — in this case, technology-assisted review (TAR), which automates and thereby greatly speeds document prioritization and review.

**SINGLE PARTNER, END-TO-END SOLUTION SUITE**

All of these sources of inefficiency and potential error are solvable with a single-partner, end-to-end solution paradigm. Here are key features of the solution offered by CSC, along with an explanation of their advantages in meeting the dual goals of efficiency and compliance:

- **Single Partner.** Our single-partner solution provides global support for all eDiscovery needs. Having one partner simplifies management and puts control in the hands of the client rather than a third party, such as legal counsel. With a single service provider, companies are able to standardize workflow into highly repeatable and defensible processes. A single-partner approach also supports preferred pricing and volume discounting. Moreover, it enables a company to build a knowledge base and to count on a partner that understands the nuances of the client’s priorities and can serve as its eyes and ears, always acting in the client’s best interest.

- **Single System.** Having multiple systems is often a source of inefficiency, and in the case of eDiscovery, it’s unnecessary. The right single-database system suite provides uniform capabilities with a rich suite of intuitive tools necessary for conducting eDiscovery in compliant fashion, with vital integration into relevant client systems. With a standard single-solution suite, staff can be trained to use the system more efficiently.
- **Elastic Cloud Infrastructure.** Delivery of eDiscovery system capabilities through the cloud eliminates the financial disadvantages of installing and maintaining systems on premises. eDiscovery software is continuing to rapidly evolve, which creates the danger of making a major capital expenditure in a system that may soon be obsolete. With cloud-based delivery, updating systems becomes the responsibility of the partner. Perhaps even more important, eDiscovery is an extremely unpredictable process, which can drag on for months or years beyond expectations — or come to an abrupt end. It would be hard to find a software capability better suited to a variable cost, consumption-based approach, which allows a client to easily scale up and, more important, scale down, as needed.

- **Globally Standardized Protocols.** Global reach means highly defensible forensic processes, compliant in all jurisdictions. It also means consistent, repeatable processes to both maximize efficiency and reduce the opportunity for error caused by hand-offs, irrespective of their global geographic location.

- **Proven Enterprise Network.** All the functions associated with a single partner and a solution suite depend on a robust network with state-of-the-art cybersecurity capabilities. CSC’s highly scalable infrastructure provides agile configuration; control over where data is processed and stored, and with whom; excellent standard security layers, with many enhancement options; and tiered storage capabilities.

Companies seeking to optimize their operations increasingly ask whether a given function fits within their core competency. eDiscovery is often clearly among the functions that do not, as some companies have found to their disadvantage. Those who place eDiscovery in the hands of specialists will significantly reduce risk and increase efficiency by taking advantage of these options, enabling eDiscovery management at an enterprise level, and even on a global scale, all with a single partner.

To learn more about CSC’s global eDiscovery solution suite, please contact us at csc.com/contact_us to have a CSC sales account executive give you more detailed information on how CSC’s services can address your company’s eDiscovery needs.

Find out more at csc.com/ediscovery.