

Avoiding The Hidden Costs Of Bargain-Priced E-Discovery

By **Michael Cousino**, Epiq Systems

Law360, New York (January 13, 2017, 4:49 PM EST) --

All organizations are looking for ways to be more efficient and save costs, so it's no surprise that many are interested in finding an electronic discovery partner who is offering a tantalizingly low price for electronic discovery services.

What those offering lower prices for e-discovery often fail to convey, however, is the final and true cost of a project that's entrusted to a bargain-priced e-discovery provider. Unforeseen coverage gaps, lax security practices, ignorance of global practices and/or delayed deliverables can all add up to a sum that's much higher than what was promised at the outset.



Michael Cousino

To avoid these pitfalls, many choose to partner with a holistic managed services provider, which can limit risk exposure and help clients save money in the long run. Here are the risks organizations run when they sacrifice quality for cost-savings:

Consolidation of Services

Small-scale or cut-rate e-discovery providers are often unprepared for the types of complications that regularly arise in litigation, forcing clients to hire additional providers to help at extra cost.

This is an example of the hard and hidden costs of cheap e-discovery. Smaller providers that end up missing the mark on estimating the true cost of a project often do so because they realize halfway through the project that they must pay for outside expertise that they lack internally.

Many firms are starting to realize they can consolidate by engaging one managed services provider for various needs, solving the multiple-vendor problem. Rather than juggling standard transactional relationships, organizations are often looking to larger vendors to meet all of their needs, from consulting providers, to software providers, to document review providers. The continuity of working with one partner to meet each of these needs streamlines operations, increases efficiency and in the long run, reduces costs.

Data Security

Another key consideration for an e-discovery provider is whether it has the resources necessary to ensure proper data security. It's ultimately a question of infrastructure rather than of expense: A

provider cannot believably claim to offer both state-of-the-art data safeguards and bottom-of-the-market pricing at the same time. When a vendor boasts of a low per-gigabyte quote, it is revealing that it likely lacks the size and buying power to afford the necessary protections for the data with which it's asking to be entrusted. For a corporate client, a breach of any data related to its legal disputes could cost it far more than any e-discovery vendor would charge.

Therein lies a double standard in how security is valued. Most companies would never consider having a startup host their email, yet e-discovery hosting is ultimately the same thing, with a potentially higher risk profile. The data involved isn't random — it's extremely valuable data that should be highly protected.

The Risks of “Just Saying Yes”

These data security issues were far less of a concern in the days when document review required little technology beyond a printer at the neighborhood copy shop. In that era, it was easy for vendors to meet clients' needs at a low cost, with little risk. The mindset of “just say yes” was established regarding clients' requests, as even modest vendors could handle clients' needs without much technological savvy or equipment.

This “just say yes” mentality is one of the biggest reasons for e-discovery price compression. The downstream change is that vendors and organizations alike underestimate security, compliance and regulatory obligations. Along with this underestimation comes a great deal of hidden risk.

Critical Security Safeguards

The industry must adapt to present-day standards. Namely, legal professionals must stop thinking of e-discovery services as a commodity — that it's a task that simply requires people with printers. It's vital that the industry become more self-aware and acknowledge that we don't have the luxury of taking these kinds of risks. Risk mitigation, regulatory compliance data security are requirements just as much as price is when you're looking to manage the highly-sensitive data involved in discovery projects.

One critical safeguard is a security event incident management (SEIM) system. This system not only monitors all attempts to access a network, but also performs behavior analysis of activity patterns, in order to quickly detect a potential breach.

With all activity monitored universally, project managers can easily detect unusual behavioral patterns. For example, if someone logs into a system unexpectedly at 2 a.m. on a Saturday, SEIM will immediately alert you of unusual activity. Therefore, if there were a security breach or compromised credentials, the incident management process can get underway much faster and in a more controlled manner. With more than 200 million events a day being tracked through such systems, this can be an expensive but extremely valuable security component.

A robust and audited SEIM system is just one example of a safeguard that all organizations should look for in their e-discovery vendors.

Global Reach

Vendors with a “cost-first” mentality also underestimate the realities of globalization and its impact on the e-discovery industry. As the borders for business continue to expand across the globe, discovery

efforts are more likely to require knowledge of multiple legal systems. For example, when a European company manufactures its products in Asia and sells them in the U.S., a lawsuit can easily involve documents from three continents. These documents are often in a variety of languages, and are subject to a different set of regulations in each country. Oftentimes, cases that can appear to be based locally can end up needing relevant data sourced from places like Hong Kong or Tokyo. When this discovery need arises, clients partnered with global e-discovery providers with multi-lingual staff and deep local jurisdictional knowledge will be able to move forward much more seamlessly.

Contingency Planning

Perhaps the most common cause behind the “hard and hidden costs” of low-budget e-discovery is also the simplest: poor planning. Unexpected setbacks can happen in the course of any project. But small, cost-focused vendors may not have the resources in place to adjust and recover, leading to extended timelines and expensive final projects. Oftentimes small providers need to prioritize certain projects, meaning some will fall off-course.

A good rule of thumb is to look for a provider that can manage unexpected project surges and extraordinary requests. This ability, along with cross-border coverage, security safeguards, managed services and other benefits often come with a large, global and diversified provider. When underpriced projects ultimately fall through, it can wreak havoc on the client and the project. Those those considering bargain-priced options should consider these risks as they assess their partnerships in the e-discovery space.

Michael Cousino is a regional vice president of e-discovery at Epiq Systems.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.