Five Reasons Why It’s Time to Disrupt Your eDiscovery Model — and Get Fit for the Future

By **Jeff Seymour**

The notion that conducting eDiscovery today means accepting unacceptable risks and costs — third-party cyber breaches, the expense of having redundant data across multiple service providers — is ripe for retirement.

How did we get to this point? At the heart of the issue is the practice of sending eDiscovery data outside of the corporate cybersecurity boundary. The unintended by-product of this arrangement is the risk of entrusting the company’s sensitive data with organizations you would not otherwise engage for that purpose.

But now there’s a way to sidestep the issue. Sophisticated organizations are recognizing that it’s possible to align around a unified, transparent security posture — one that can address the priorities of all constituents, protect business continuity, and amplify the organization’s strategic successes in an environment that continues to hold surprises.

From a provider-centric model to a security-centric one

The characteristics of eDiscovery lend themselves naturally to the engagement of outside support: it’s episodic; it requires expertise across a broad range of skills; it calls for objectivity; and it’s not strategic to a company’s mission — it’s a necessity. Thus, activating a panel of litigation services providers (LSPs) or law firms to support eDiscovery processes is typical.

While outsourcing those services has historically proven to be effective and cost-efficient, recent, highly publicized breaches have laid bare the structural vulnerabilities inherent in relying on security operations of the provider-centric model. Consider that a company with multiple matters has extremely sensitive data resident at multiple providers — with no centralized view, no consistency and no overarching security framework in place. The safety of that disparate data is in the hands of a patchwork of providers, programs and employees — over which the company has little visibility and even less control.

Meanwhile, as cybersecurity, privacy and business resilience continue to rise up the list of most critical corporate concerns, the roles and responsibilities of CISOs and CROs have continued to grow. Over the last few years, the overwhelming majority of corporates have moved their business productivity platforms to versions that are backed by the provider's public utility cloud — which can also serve as the backbone for their eDiscovery platform.

Thus, many legal departments — simply by hewing to their longstanding stable of litigation support providers — have suddenly found their security posture to be off-strategy, potentially raising their exposure for any future incident. (After all, if the approved environment for the company's unstructured data is in one cloud provider, why take some of the most sensitive data out of that environment and push it somewhere else for eDiscovery?)

Why eDiscovery should be executed like a disaster recovery plan

In eDiscovery, speed, completeness, accuracy, security and efficiency must be front and center. Yet the ramp-up process of engaging external counsel, finding a technology vendor, identifying experts, agreeing on data-transfer logistics, meeting platforms, knowledge repositories, etc., can take days (if not weeks) — and time is of the essence.

Consider a regulatory investigation triggered by a whistleblower letter. Under the traditional method, the company will first digest and set up the matter, then meet with external counsel to discuss its ramifications. External counsel then contacts an LSP from its provider panel. Each provider must then sign an engagement letter, and fill out a 400-question security questionnaire. Once the selection is made, the next step is to meet with the company's IT specialists to try to locate all relevant data.

Even under the best of conditions, this start-up process is inherently inefficient.

By contrast, if you use an advanced SaaS eDiscovery service on the front end, in a matter of just a few hours, all relevant data can be collected, organized and ingested into a secure cloud-based Relativity instance. And, just as in a disaster recovery scenario, when roles and expectations are clear and the process is streamlined, speed and accuracy are enhanced, which can materially affect the outcome.

Another advantage of working this way: you can take direct ownership and governance of the platform without having to run and administer it — ensuring flexibility and security, while maintaining full control of your data at all times.

Constructive disruption: The top 5 reasons to transform your eDiscovery process

Make a break with traditional discovery practice, and switch to an advanced, SaaS operating model capable of baking sophisticated data governance into the process. Here are five reasons why it's time to disrupt your eDiscovery model — and get fit for the future.

1 Flexibility

Effective governance, and the operational flexibility that it enables, begins and ends with control: keeping your data from flowing outside the corporate IT boundary to third parties, maintaining a centralized platform for data hosting — and enjoying full visibility into both matters and costs. A SaaS solution that keeps *you* in control of your data enables you to decide which matters to work on in house, and which to share with third-party providers.

2 Security

Wherever there's data, there's cybersecurity and privacy risk, and there can be no safe haven within the organization for such risk. Your eDiscovery solution must be part and parcel of an enterprise-wide security posture, be it within your own framework — or ideally that of a sophisticated managed security service with a robust global infrastructure capable of quickly detecting and responding to anomalous behavior.

3 Efficiency

End-to-end workflow automation gives you the agility, processes and technology you need to quickly handle any matter — no matter how urgent — from identification through review through production. It also enables you to connect your corporate systems to further enhance the process. A SaaS platform with native integration capabilities can also help you triage and optimize the amount of human intervention needed, minimizing your overall spend.

4 Centralization

When all your eDiscovery data sits in a central repository, you can stop relying on a plethora of serial custodians to handle all the matters that come your way every year — especially valuable if you operate in a highly regulated or highly litigious industry. Consolidating your hosting environments not only reduces third-party or privilege risk while giving you visibility into the full lifecycle of all your discovery operations (including timely, consistent metrics) — it also gives you predictability and more control over your spending.

5 Value added

This modern eDiscovery approach enables you to integrate other data sources or systems directly, unlocking potential value-add benefits through advanced data analytics, threat detection and other techniques. It can also remove historical barriers to use of the platform for adjacent use cases, such as DSARs response, LIBOR remediation and contract remediation.

With the triple stakes of legal outcomes, data security and cost efficiencies on the line, it's never been more urgent to find a comprehensive, secure and future-proof information governance system. The good news is that this new strategic way of handling eDiscovery can not only address the needs of the broader team at the table — from Legal to Risk to Information Security to CFO — it can also make the organization more flexible, more efficient and more resilient.

So make a virtue of a necessity, and disrupt your eDiscovery practices — before they can disrupt you.

Looking for ways to regain control of your eDiscovery data and spend? Contact our team to find out how we can work together:

Jeff Seymour
Principal, Cybersecurity, Privacy & Forensics, PwC US
Email
Tel:+1 212-603-9411

Philip Upton
Principal, Cybersecurity, Privacy & Forensics Digital Solutions leader, PwC US
Email
Tel:+1 646-244-4374

Dave Rogers
Director, Cybersecurity, Privacy & Forensics PwC US
Email
Tel:+1 817-726-3806

© 2021 PwC. All rights reserved. PwC refers to the US member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.