When Discovery Goes Bad: The High Cost of Poor Electronic Discovery Practices

Corporate electronic discovery, or eDiscovery, costs are ballooning. Borne out of civil litigation and government investigations, eDiscovery refers to the process of producing e-mails and attachments, instant messages, and any other electronic records, on request, within a tight timeframe, and from every nook and cranny of the corporate IT and physical environments.

The discovery process itself is nothing new. In the days where paper content was king, lawyers started the discovery process by interviewing witnesses and requesting relevant documents which were produced, numbered, and delivered. It was all very manageable and civilized.

Then came the digital explosion.

Today's lawyers must deal with a huge universe of data and its attendant challenges: massive tape archives, data deletion anxieties, litigation holds, semi- and unstructured data, and broad-based discovery requests. These issues combine to make eDiscovery extremely expensive to carry out, with an even higher price tag for failure. (For a true horror story of eDiscovery gone bad, read the sidebar "Morgan Stanley Has a Very Bad Day")

Massive tape archives. Enormous eDiscovery problems arise from trying to search massive tape archives. Tape is a disaster recovery tool and not an archive medium. Nevertheless many companies keep huge volumes of archived data on tapes. When a company must return to the tape to collect discovery data, they face a huge universe of largely irrelevant data and a lack of tools and manpower to search it. Realizing how expensive an internal eDiscovery process will be, many companies try to solve the problem by shifting the whole mess over to their outside counsel, who will go over it with a fine-tooth comb – charging by the hour. This becomes an extremely expensive proposition.

Deletion anxieties. Another complication is that companies are afraid of inadvertently destroying data lest they be accused of destroying evidence. This is less likely to happen if a company already had a sensible data deletion policy in place and can prove that it followed it faithfully without breaking litigation holds. But few companies will do both things. Remember Enron and Arthur Andersen? Arthur Andersen had a deletion policy in place but did not consistently follow it. When company lawyers tried to trot out the deletion policy after Enron documents were destroyed, the judge didn't buy that selective choice.

Affirmative notices and litigation holds. Government regulations like Sarbanes Oxley list strict retention requirements, and also changed notification and retention periods for upcoming discovery motions. Traditionally, if a subpoena was not yet issued but data had

passed its retention period, the company could delete it without penalty. But now companies might receive an affirmative notice six months or so before the subpoena, directing them not to destroy any evidence that might be requested in discovery, even if that data's retention period is up. The civil world has a similar process called the litigation hold.

Semi- and unstructured data. Discovery data is found not only in structured databases but in semi-structured and unstructured documents like e-mail, word processing, spreadsheets and presentation data. Not only are there mounds of information to go through, there are many different places where IT must look to return the requested information to the lawyers: network shared drives, individual users' hard drives, backup tapes, archive disk.

Broad-based discovery. Smart government investigators like Eliot Spitzer of New York tend to issue broad eDiscovery requests, having stumbled onto some massively smoking guns in electronic messages. The same trends exist in civil litigation where very expensive broad-based eDiscovery requests are becoming more common. When the lawsuit involves two companies, broad-based discovery is not a large issue because the defendant can turn right around and ask the litigating company for broad-based discovery of its own. But if an individual is suing a company he can ask for broad discovery, and the company will likely often have to comply. An example of a broad-based discovery from an individual against a corporation is the successful suit filed by Carol Ernst against Merck claiming that her husband's 2001 heart attack was related to Vioxx. Ernst just had to produce her late husband's medical documents, but Merck had to spend huge amounts of money to locate and produce its related documents. And on top of that, it lost the case.

eDiscovery Strategy: More than Survival

To survive eDiscovery – even to profit with a proactive strategy – companies must treat discovery from a process perspective: a cross functional and repeatable business process across a portfolio of cases. Such a cross functional and repeatable business process involves both Legal and IT. It starts with a repeatable process to document that the company is taking good faith and reasonable steps to protect the information being held for future discovery.

eDiscovery and Legal. Even before a case is filed, the company lawyer should generate communications to all witnesses that they have an obligation to preserve certain information for possible collection and not to delete it even if the retention period has passed. The process must also maintain a chain of custody so the company knows and can prove where information originally came from, which requires preserving metadata associated with the data. Legal must also be able to give IT clear directions, guidelines and expectations for discovery.

eDiscovery and IT. To do its job in discovery efforts, IT will require the right tools to powerfully manage corporate semi-structured and unstructured content, to search, automate collection, and establish a platform to handle legal holds and efficient data

organization. This requires moving to disk-based archives, since there is little ability to search by individual messages or to use policies on warehouses of backup tapes. By using disk-based archives, IT can establish a searchable repository to automate data collection by keyword and other bases, ending up with a focused, accurate and complete set of relevant data. This saves upfront money and time, greatly decreases the cost of penalties from a poor eDiscovery response, and coincidentally grants access to valuable historical data.

This process requires a systematic approach containing not a single solution but linked solutions for a comprehensive strategy. Consider working closely with professional services consultants who are experts in content management and eDiscovery, and begin with corporate assessments to establish priority needs and project timelines.

Primary components should include integrated email archiving, content management, federated search, and CAS (content-addressable storage). Email archiving and content management software place data into a searchable repository, while federated search goes across all repositories and pulls relevant data into CAS. The archived data on the backup drives can be safely deleted according to named retention periods, because a copy of the data is locked onto the CAS for legal discovery at a later date. CAS also serves compliance purposes by maintaining metadata histories including migration and modification dates, and tracking and locking out file modifications. Email management should include policy-based retention and disposition of corporate records, and online access to e-mail records management with assured authenticity.

A working eDiscovery process is not merely reactive; it is also proactive with strong benefits to corporate ROI. Successful eDiscovery requires intelligent content management, which itself has great business value including improved historical value from well managed archives, IT and Legal time and manpower savings, greatly reduced eDiscovery costs, less risk of penalties and criminal actions, and a powerful and cost-effective tiered storage strategy.

Sidebar: Morgan Stanley Has a Very Bad Day

As proof of how costly poor eDiscovery practices can be, you need only look to hapless Morgan Stanley.

Judge Elizabeth Maass told the investment bank to pay a full $604.3 million claim made against it by billionaire financier Ronald Perelman, plus $850 million in punitive damages. The nature of the damages? Morgan Stanley repeatedly failed to produce emails that were vital to Perelman's suit.

Perelman's attorneys had asked for emails dating back to 1998. Morgan Stanley protested against the broad and expensive discovery exercise, but Judge Maass told them to do it

anyway. The bank was in the middle of transferring a tape archive of 300 million emails onto more easily searchable disk. But the project was incomplete, and much of the requested information was still on backup tape. Not only was tape resistant to search tools, but thousands of Morgan Stanley's backup tapes were languishing in odd corners and closets – literally.

Morgan Stanley's IT executives told the judge that they had searched everything anyway. But in May 2004, a staff member found 1,423 backup tapes in a storage cupboard in Brooklyn; an additional 129 tapes showed in Manhattan, and yet another set were discovered in the bank's headquarters soon after.

In addition to the lost tapes, Morgan Stanley had no documentation on how to search one of its largest tape archives, searches on another archive turned out to be case-sensitive, many of the tapes couldn't be opened because their format was obsolete, and the search tool simply would not search a significant number of attachments. All in all, a textbook case of how *not* to run your archive program.

Judge Maass didn't like it one bit and penalized the bank accordingly. The jury award plus the punitive damage fees totaled a whopping $1.45 billion judgment against Morgan Stanley.