Craig S. Mullins

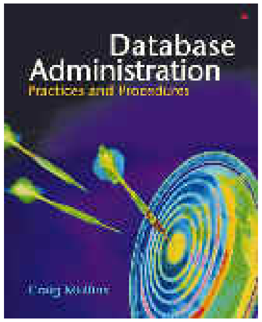
Return to Home Page

May 2007

DATABASE
TRENDS AND APPLICATIONS

The DBA Corner

by Craig S. Mullins



The Impact of e-Discovery on Data Management

If you’ve been head-down, in-the-trenches you might have missed the sweeping changes being thrust upon the data world due to regulatory compliance. And even if you’ve noticed, chances are that the sheer volume and nature of the regulations were too mind-boggling to fully digest. This month, I'd like to discuss a few of these issues that will impact your databases and data management policies.

First of all, ensuring compliance requires a collaborative effort between business users, IT, and your legal department. This can prove to be a challenge because these three disparate groups are quite distinct and rarely communicate collectively. IT talks to legal only when they have to – and that is usually just to get approval on contract language for software purchase. IT and business communicate regularly (at least they should), but perhaps not as effectively as they might. But all three are required:

- **Business**: must understand the legal requirements imposed on their data and systems as dictated in regulations

- **Legal**: must be involved to interpret the legal language of the regulations and ensure that the business is taking proper steps to protect itself

- **IT**: must be involved to implement the policies and procedures enact the technology to support the regulatory mandates

So we need to map and categorize our business data in accordance with how it pertains to regulations. Once mapped, controls and policies need to be enacted that enforce compliance with the pertinent regulations. This can require better protection and security, enforce longer data retention periods, impose stricter privacy sanctions, mandate improved data quality practices, and so on.

One of the looming issues facing data management professionals is preparation for e-discovery. Yes, regulations mandate that we retain data longer, but there are rules for producing the data that is retained, too. I mean, why keep that data around if there is no need ever to see it again?

The ability to produce retained data upon request is typically driven by lawsuits. You probably can recall examples of courtroom showdowns on television where truckloads of paper documents were required during the discovery process of the lawsuit. But times have changed. Increasingly, the data required during the discovery process is electronic, not written. That is, it is stored on a computer and much of it is stored in a database management system.

Which brings me to the Federal Rules of Civil Procedure (FRCP), which are the rules used by US district courts to govern legal proceedings. One of the items in this set of rules dictates policies governing discovery. Discovery is the phase of a lawsuit before the trial occurs during which each party can request documents and other evidence from other parties or can compel the production of evidence. You might remember seeing movies or TV shows where the discovery process required the prodcution of boxes and boxes of paper. Today, this would be e-discovery in that the form the evidence is computerized data. So, for IT and data professionals, it is very important that we understand the legal process of discovery as it pertains to electronically stored information.

The FRCP underwent some changes in late 2006. Rule 34b of the FRCP was changed to state that "A party who produces documents for inspection shall produce them . . . as they are kept in the usual course of business..." So clearly this change compels organizations to improve their ability to produce electronic data.

And Rule 37 of the FRCP adds a new section, Rule 37(f), which provides a safe harbor from sanctions arising from spoliation. According to this section, "absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information as a result of the routine, good faith operation of an electronic information system." Basically, this section shines a spotlight on the need for organizations to develop a clearly articulated, well-executed, and uniformly enforced records retention program (that should include database data). Doing so will offer some level of protection from "adverse inference" rulings arising from spoliation.

And there are likely to be additional implications arising from the changes to the FRCP, especially when coupled with the growing list of data breaches and the growing regulations being voted into law by federal and state government. It means that we will be forced to treat data as the corporate asset that it is - instead of just saying that we treat it that way. That means analyzing and modeling data and metadata, maintaining and managing data and metadata, and archiving it for long-term data retention.

This should be good news to all the data bigots out there. The laws are finally catching up with what we knew our companies should have been doing all along.

From Database Trends and Applications, April 2007.

Home.