Craig S. Mullins

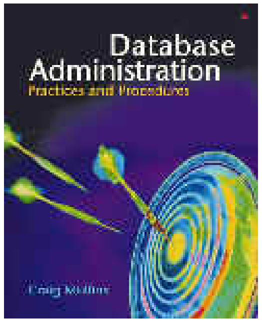
Return to Home Page

May 2008

DATABASE TRENDS AND APPLICATIONS

The DBA Corner

by Craig S. Mullins



The Cost of a Data Breach

If you read the It press these days you know that data breaches are quite pervasive. We keep hearing about data being lost, stolen, and nefariously accessed. It is all enough to give a data professional a throbbing headache. But what is the actual cost of these data breaches?

Most certainly, everyone can agree that a data breach is a bad thing and that we all should be doing a much better job of protecting our data than we are doing. And by we, I mean all of us, not just corporations. Individuals who are entrusted by their employer to protect, access, and manage data need to step up and ensure that data and database security is properly implemented.

This means that we need to imbue our everyday actions with a sense of data protection. And that requires a change in mindset. Historically, DBAs were not very interested in database security. Oh, they would try to ensure that the appropriate authority was granted to the appropriate user, but little more than that. Indeed, when new versions of the DBMS came out, many DBAs would just rifle through the new documentation ignoring the security features on their way to reading about performance issues. This has changed somewhat, but it needs to change even more. Database security and data protection must become more ingrained in the practices, policies and procedures used by DBAs to manage their database infrastructure. Think about it; if more change were not required would we still be hearing about a new data breach every week?

How bad is this problem? The Privacy Rights Clearinghouse keeps track of every data breach that is reported. According to their research, more than 218 millions records have been breached between January 10, 2005 and March 15, 2008 – over the course of more than 500 separate breaches.

So the numbers indicate that the problem is quite real and represents a substantial issue that need to be dealt with. But can we put a price tag on all of that unprotected and lost data?

Evidently, we can. Forrester Research conducted a survey of companies that had experienced a data breach which concluded that the average security breach can cost a company between $90 and $305 per lost record. But coming up with a precise figure can be difficult because of the additional, extenuating circumstances surrounding data breaches. The cost needs to factor in such details as the expenses of legal fees, call centers, lost employee productivity, regulatory fines, customer losses, stock losses, and the nebulous cost of bad publicity.

I am not a fan of relying on a single data point for anything as serious as the cost of a data breach, so let’s take a look at an alternate study. The Ponemon Institute conducted a study of data breaches in 2006 that pegs the average cost per lost customer record at $182. This matches up reasonably well with the Forrester Research report. If you are still skeptical, you can always roll your own numbers using the free web-based data loss calculator provided by Darwin Professional Underwriters, Inc. at http://www.tech-404.com/calculator.html.

OK, so what do we make of all of this? Well, the obvious point is that data breaches are costly, even at the low end of Forrester's range - $90 per record. Consider a recent data breach case from February 27, 2008 in which Health Net Federal Services reported thousands of doctors in eleven states had their personal information (including social security numbers) openly posted on a company website. According to the Privacy Rights Clearinghouse, the total number of records involved was 103,000. So what did that cost? At the low end, the cost is $9.3 million, but at the high end it balloons to over $31.4 million. Using the Ponemon estimate, which is sort of in the middle, the cost is $18.7 million.

So the cost of a data breach can be quite steep. As such, it makes sense to spend some time and money up-front to better secure your data... and also to spend some time and money being able to monitor and audit access to your databases and systems.

From Database Trends and Applications, May 2008.

Home.