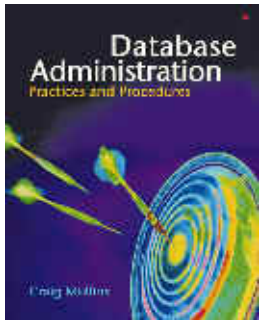
Craig S. Mullins

Return to Home Page

June 2006



The DBA Corner

by Craig S. Mullins

Do Data Security Breaches Require a Data Professional's Oath?

A couple of months ago I wrote about data security in this column. This month I am writing about a related topic – the increasing instances of data breaches and what must be done about it.

A data breach is when an unscrupulous person nefariously gains access to data. It usually involves hacking into a site that is not properly protected or stealing equipment with unprotected data on it. Of course, sometimes data security and privacy is violated without a breach. Maybe sensitive data is exposed on the web for all to see; or a company's data privacy policy is written in such a way that it protects the company instead of your data. At any rate, there continue to be numerous instances of data breaches and precious little being done about them.

In just the past couple of months the following stories have been reported in computer journals and newspapers across the nation:

- A database problem with a DiscountDomainRegistry.com, a U.S.-based domain name registrar exposed sensitive financial and personal information relating to thousands of domain name registrations.
- An employee at Progressive Casualty Insurance Co. accessed information on foreclosure properties she was interested in buying. Although the employee did not hack into systems to access the data, it was accessed and used improperly.
- Personal information of Florida state employees may have been compromised during offshore work conducted on the state's payroll and human resources system. Over 100,000 current and former employees who worked for the state during the 18 month period of January 1, 2003, through June 30, 2004 may be impacted this breach
- The personal data of perhaps millions of current and former Florida residents were made available to anyone with Internet access. The sensitive information includes Social Security numbers, driver's license information and bank account details.

Evidently even the Internal Revenue Service thinks it is just fine if tax preparers are allowed to sell your tax return data and information. The IRS has taken steps to change the rules regarding the privacy of federal income-tax returns. The changes, proposed in December 2005, would allow accountants and other tax-return preparers to be able to sell information from individual tax returns to marketers and data brokers.

The attacks and data security breaches in the news come in many forms. One type of attack is where an organization allows personal financial data to be surreptitiously accessed or stolen. Modern organizations are going to have to come up with better methods of protecting "their" data. And I place "their" in quotes because it is not really theirs, but ours (meaning, the customers of these companies). We share our data with organization under the assumption that the organization will be a good custodian of that data. Often, this is a bad assumption.

As such, more government regulations are in the works to enforce better data governance. For example, the US House of Representatives is doing something. In late March 2006 the U.S. House Energy and Commerce Committee passed legislation forcing data brokers to disclose security breaches to the public. The Data Accountability and Trust Act (or DATA) would place new requirements on data brokers to notify the public if there is a "reasonable risk" of identity theft associated with a data breach. I think this could be a good first step. This, I believe, is a good thing, but it is just the beginning of what will be necessary to control inappropriate data access.

As data professionals, many of us are just cogs in the machinery. But we need to become cognizant cogs! By that I mean we need to become better informed about what our employer's are doing to protect data. Even further, we need to make sure that it is an acceptable use to which our employer's are putting that data.

If we don't do it, who will? Do you trust the government to get it right? What happens when it is the government that is abusing data? This problem is not going away. Solutions, though, are slow coming – especially when it involves something nebulous, like ethics and morals.

Maybe we need a data professional's creed like the Hippocratic Oath that doctors take. Maybe something like this:

I give my word to keep according to my ability and my judgement, the following Oath.

"To consider dear to me the trust placed in me to faithfully protect and be a good steward of the data and information with which I come in contact. I will enact proper procedures and security for the good of my company's customers according to my ability and my judgment and never do harm to any data entrusted to me.

To please no one will I cause any data to be breached nor will I give advice which may cause a data breach.

All that may come to my knowledge in the exercise of my profession or in daily commerce with men and companies, which ought not to be shared, I will keep secret and will never reveal.

If I keep this oath faithfully, may I enjoy my life and practice my art, respected by all men and in all times; but if I swerve from it or violate it, may the reverse be my lot."

Of course, to be truly useful such an oath would require a organization (such as the AMA backs doctors) to support and guide IT professionals. Is that a reasonable thing to expect of data professionals? What do you think?

From Database Trends and Applications, June 2006.

Home.