

# DATABASE

## TRENDS AND APPLICATIONS

Solutions for the Information Project Team • [www.dbta.com](http://www.dbta.com)

Volume 22, Number 2 • June 2008

# Q&A

## Industry Leader Interview



**Rajesh Parthasarathy**  
President and CEO  
MENTISoftware

## IT Security Requires a Collaborative Approach

*MENTISoftware offers security solutions for companies using Oracle-based systems and is adding support for an expanded range of ERP suites and database platforms. DBTA talked with Rajesh Parthasarathy about why top management cares more than ever about protecting sensitive data.*

### **DBTA: What new pressures are affecting companies' approaches to data security?**

**Parthasarathy:** Security is becoming more of a business issue than a core IT issue. There are multiple reasons for this, which are primarily based on concerns about the bottom line, market capitalization, and the brand and reputation. Companies work hard to get the market capitalization up by 10 percent. That can be lost overnight if they have a bad data breach or data loss story. And the brand loss and reputation loss with customers and with vendors and partners is also another driver causing security to become more of a business-oriented issue.

### **DBTA: Is this new?**

**Parthasarathy:** This change has been coming for awhile but only now over the last six months to a year is when it has actually started boiling up to the business side of the equation. Business stakeholders want to get more involved in IT, in security. They want more visibility into the overall IT process. A big part of the reason is that applications were built in a more naïve time when we were building applications to get different parts of a business into a single system; we wanted to automate

processes, we wanted to make our business more agile by getting everyone onto an enterprise resource planning software like SAP or Oracle.

### **DBTA: So, what has changed?**

**Parthasarathy:** When those applications were engineered, security and compliance and risk were really not in the forefront of the thought process or architecture. Subsequently, when we started realizing that we have made a single point of attack or single point of failure, there was a need to put in some IT controls and security controls that can be used by a DBA or developer or some really strong IT folks. But, that goes against separation of duties. If the core IT folks like the DBAs and developers have access to too much data, empowering them with the tools to protect the data perpetuates the problem. It doesn't necessarily solve it. IT, Audit, Compliance and Security - any one of these departments alone has very little visibility on what is happening on the security side, because they each only have a piece of the puzzle. All of these stakeholders together will see the entire picture.

### **DBTA: How big a concern are privileged users?**

**Parthasarathy:** The FBI and CSI [Computer Security Institute] jointly put together a security survey every year and over the last three or four years, the insider threat numbers have been becoming the largest reason for data theft. "Insider" meaning anybody who has a legitimate access to your networks and your environment. I think the 2007 survey showed

that about two-thirds of all data loss incidents or data breaches happened through insiders. Now, that is not all malicious - a significant portion of that is also negligence and also bad processes and lack of controls.

### **DBTA: What can business stakeholders do?**

**Parthasarathy:** We provide this service called SOS - the "state of security" service - where we work with a company and review the entire database security posture from where the database is installed, who has access to it, and so on, and we give best practice recommendations and compliance recommendations. Established process is a piece of code gets written by a developer, it gets moved to user acceptance testing for the functional users to test the code to see if it matches needs and requirements, and then it gets migrated to production. We have been recommending a step in the middle where the security, compliance or audit officer reviews every piece of code to determine if this is going to change the risk matrices or cause additional compliance problems. I have been in environments where we ask a developer to make a payables report that just lists vendors and vendor balances, but the developer takes the liberty of filling an empty space with the vendor tax ID number and address, just so it can be used at a future date - maybe. But what happens is, if you have individuals as vendors now you are suddenly out of compliance with all of the breach notification laws. Your payables clerk now gets access to Social Security numbers.

### **DBTA: What is needed?**

**Parthasarathy:** We have been talking about a more collaborative approach, a more business-focused approach for security and compliance for four or five years now.

### **DBTA: How is your approach different?**

**Parthasarathy:** Our approach is different from any other company - in that, traditionally, solutions have been point solutions only core technology folks could use. It was a DBA tool or a developer tool or it was something only somebody with strong IT skills could use - and that pretty much eliminates the security, compliance and the audit officers from participating in the process. How we approach this is: let us first help you determine where sensitive information is stored in your databases, then we will show you which parts of an application actually expose that sensitive information, then we will take the next step of figuring out where your exposure is - who has access to this information. Once you have that intelligence, then you can use our rules-based products to prevent or detect inappropriate access at the production database level, at the non-production database level and at the production application level.

### **DBTA: So, what does this enable?**

**Parthasarathy:** By taking that approach we have been able to automate your entire security and compliance needs as far as protecting sensitive information, and it is all built using a data classification engine so a security officer can understand where in the database PCI information is stored, which parts of the application expose it, who has access - is it appropriate - and take action.

### **DBTA: You can tailor your approach to specific industries.**

**Parthasarathy:** Exactly. What our data classification enables our customers to do is

build templates to hone in on specific business areas or compliance areas. We have customers that have to comply with HIPAA and they are able to build a template with different data classifications that gives a list of different tables that contain HIPAA-related information. From there on out, it will flow through the rest of our products. You can do the same thing for PCI data security standards. We have customers that use our application for the personally identifiable information that all those breach notification laws cover. And because we have pre-built all the data classifications and also provide a data classification engine to extend our application, companies are able to turn around and build templates in a matter of days.

### **DBTA: What is new in the 6.0 release of MENTISoftware's GRC portfolio?**

**Parthasarathy:** Our framework and our modular approach have always been available but now with this new release, the integration points are better, there are more wizards and it is a lot easier to use. And with our basic mantra of trying to empower business to participate in the security and compliance programs, our products are more business-oriented than pure IT-oriented.

### **DBTA: What else?**

**Parthasarathy:** We have a lot of business-driven interfaces so customers can really start achieving the security goals very easily. All of these products are standalone products built on a common framework but they also share a lot of information. New for this release, you can build a template of all of your personally identifiable information, from there you can go to the next product, iCatalog, and say, "now show me which parts of my application expose this data." From there you can jump into iAudit and say, "show me who has access to that information at the application level." You can jump

to iDocument and say, "show me who has access to this piece of code in the database" - and this is all integrated. It lends itself to a logical flow through your overall risk management program.

### **DBTA: Can a CEO or president look over the shoulder of a data security expert?**

**Parthasarathy:** Absolutely. If I am a CEO and I know that I am getting a lot of heat for PCI compliance, I can say, "show me who has access to this information," and "show me what security methods have been deployed on my different applications and databases." You can very quickly get a very good sense of that.

### **DBTA: What's next?**

**Parthasarathy:** We are rapidly evolving into other ERP suites. We are doing Lawson and PeopleSoft in the upcoming release, which is slated for this quarter. The next quarter we have SQL Server and EnterpriseDB integration, and then the last quarter we are also going to other databases like DB2. We are growing broadly and deeply at the same time. We are going to multiple ERPs, multiple database platforms and this is all happening at a very, very rapid pace.

### **DBTA: Many companies have heterogeneous environments.**

**Parthasarathy:** Right - and some of our customers use these heterogeneous databases in a very complex manner so there are some downstream implications. Our iScramble product that protects information in non-production databases by actually scrambling the data is also intelligent enough to downstream it into these other databases. There could be Oracle E-Business Suite database that stores some information that is used in downstream SQL Server or DB2 databases. That is also a big driver for us to move to these new database platforms.