FOUR HUNDRED Stuff

Hardware, Software & Services

REPRINTED FROM VOLUME 11, NUMBER 28 – September 6, 2011

Field-Level Encryption Handles Security Compliance for Collections Firm

by Dan Burger

Data encryption has taken on a much larger role in IT departments ever since the protection of sensitive and confidential information became a high priority for so many companies. We hear a lot of complaints about regulatory compliance, but without it your personal information is an easy target for those with criminal intentions. For many IBM i companies, the question is not about whether to encrypt data, it's how to encrypt data. A good example is Bass & Associates P.C., a law firm providing national debt recovery services.

Financial institutions have really felt the heat of regulatory compliance. They handle data that criminals covet: bank accounts, credit cards, and Social Security numbers directly tied to plenty of personal or business information. Bass works in this arena. And because you're reading about them in *IT Jungle*, you know there's an IBM i (or perhaps an IBM System i, iSeries or AS/400) playing a mission critical role in the business.

Bass is a collections and bankruptcy firm that contracts debt-recovery services to companies in the credit-granting industries. It provides professional portfolio management for consumer and commercial debt, which includes student loans, bankruptcy, collateral liquidation, litigation action, and probate services.

Its technology-intensive automated system relies on two Power7 servers running IBM i 7.1. And it meets regulatory compliance security obligations using field-level encryption software from Linoma Software, a company that specializes in protecting sensitive data and automating data movement. Linoma has more than 3,000 customers around the world, including Fortune 500 companies, non-profit organizations, and government entities.

The communications network at Bass stretches beyond its customer base and includes accesses to major credit bureaus, bankruptcy and civil court records, and various government databases.

The IT department consists of a six-person staff that's responsible for maintaining and implementing the Bass networks, servers, and applications. The core application is a recovery management system (RMS) by FICO (formerly known as Fair Isaac Corporation).

When Ian Atkinson, chief information executive at Bass, started hearing from customers that security audits were pointing out that sensitive data needed to be protected in the database and throughout each company's network, he began to research encryption. At that time, the core business was run on an iSeries Model 810 production box with a System i Model 520 as a high availability backup. The leases on both boxes were expiring.

"We started the project in April 2010 with enquiries to vendors, including FICO's plans for the RMS product," Atkinson said. "We looked at this search in terms of the needs of our clients and also our desire to protect our own sensitive data."

Initially, full disk encryption was being considered as a possible option. However, it was determined to be unnecessarily complex involving multiple logical partitions, the modification of applications, and it did not allow field-level data masking, which was desirable feature for Bass.

"The field-level encryption in Linoma's Crypto Complete gives us the advantage of allowing the encryption to occur at a more granular level," Atkinson explained. "For example, it's easy for us to control which internal users at Bass are greatly limited in the amount of data they can see, which ones have certain data partially masked, and which employees get to see all the data."

This field-level data masking feature in Crypto Complete is backward compatible to the V5R2 version of the operating system, but only users of IBM i 7.1 can take advantage of the DB2 field procedure feature that allows encryption and decryption of data to occur without program changes. That enhancement is not just convenient; it's a time saver that avoids code manipulation.

It was a fortunate coincidence that Bass was ready to make a hardware upgrade, which carried with it an OS upgrade to IBM i 7.1, allowing the company to use the new DB2 field procedure feature right away.

During the hardware and operating system upgrade there were four machines in use, Atkinson explained. That included the old production and backup machines and the new production and backup machines. MIMIX high availability from Vision Solutions was being used to replicate data on both the old and new servers and the machines were running in parallel.

"At that juncture, I could only test the DB2 field procedures in Crypto Complete on 7.1," Atkinson said. "I could not do any production encryption until we upgraded to the new boxes."

"One or more fields in a database file can be targeted for encryption and can be activated at one time," said Ron Byrd, senior software engineer at Linoma. "When the customer is ready to activate the encryption, they just need to make sure no users are in the targeted files in order to maintain their integrity. The files will then get locked and all the existing values will get encrypted during the initial activation. After the activation, the files are unlocked and are ready again for use. Then any new or changed field values will be automatically encrypted."

When the migration to the new Power7 servers running IBM i 7.1 was completed--which was not a difficult task after running the old and new systems in parallel for several months--it was encryption time.

Typically you would expect to read that absolutely nothing went wrong and then you'd begin to doubt the credibility of this story. Both Atkinson and Byrd, however, talked about a glitch. In the midst of moving to a new OS and working out high availability issues along with incorporating encryption, the HA target server was balky about getting in synch.

After a couple of days, the kink was ironed out with a patch from Linoma and a PTF from IBM.

"If I were to approach this same encryption implementation today, I'd say it could be accomplished in two to three hours," Atkinson said.

Part of the FICO application presentation at Bass is a Windows-based client front end and auxiliary pieces of the system are built for browsers. Because the encryption is applied to the database, there's automatic field decryption/masking even when the data is accessed through the browser. The same is true for data that's downloaded to spreadsheets using ODBC connections, because it is decrypted automatically with the same masking parameters.

Atkinson is very satisfied with the outcome. He describes the project as "a key component in our security strategy and compliance strategy."