Dialogue

# Records management: Don't be distracted by SOX

*ABABJ spoke with Van Carlisle, CEO of Fire King, a security and records management group based in New Albany, Ind., with expertise in paper and digital documents. Carlisle believes that when it comes to data management, executives must develop a strategic approach—thinking both in terms of the "big picture" vision and the details of storage. He suggests one method of organization: vital records protection, and explains his reasoning here.*

**In the white papers you've written you remind readers that records need to be distinguished from each other in order to create a workable storage method. Why is that important?**

Not all records have the same value to a firm. To be distinguished as "vital," a record must contain information that is essential to the organization in the event of a disaster. Also, records regarding certain key business transactions need to be saved for legal and other reasons that materially impact the firm's risk profile.

**The heavily regulated banking industry has always had a pretty good grasp of its information, in the largest sense, wouldn't you agree?**

Yes, the banking industry is fairly careful. Best practice leaders have long had effective ways of keeping their data and records, both electronic and paper-based, safe.

However, you always have businesses in all industries that rely on keeping paper records piled away in boxes or in poorly organized filing cabinets, and, in the case of electronic records, on tape drives, which aren't easily searched. With regard to the banking industry, my bigger point is that there will be a higher standard of records maintenance given the new regulatory climate, particularly with Sarbanes-Oxley, which is being interpreted broadly regarding records protection.

Companies will need processes and controls in place to mitigate compliance and legal risks.

**Do you have any specific advice about handling SOX requirements with a records management system?**

When you make records searchable, you make them easier to interact with and, in the larger sense, easier to validate. You can say, "I stand behind these financial records," because you can find all the supporting line item detail easily and quickly.

**What other points about records management do you emphasize in your work?**

Yes. Records management, as a discipline, tends to pertain to infrastructure issues like the durability of the medium, the ease of retrieval, or when and how to destruct older records that no

**DIALOGUE,** continued on p. 60

extensive staff, and huge base of supporting vendors are all guided by an industrial strength policy that is distributed on the intranet. Others in the vast "middle market," struggle to give a less than ideal policy more than nominal play.

Another source agreed that good policy still appeared in an uneven distribution in the financial services industry. "Sometimes we see things that are pretty shocking," he said.

### What policy can do

M-Tech customer Charlie Dixon, vice-president technology, with $6 billion assets Riggs Bank, Washington, D.C., says his bank, for one, has stepped up many facets of its policy since 2001, prior to the bank's much publicized Bank Secrecy Act troubles.

It has also made numerous tech purchases, including use of an incident tracking system and adoption of M-Tech's password management technology—decisions partially guided by needs that policy revealed.

"We take policy seriously here," Dixon explained. "It is relevant, it is regularly updated, and it is referred to during application development, for instance."

Policy makes a difference in matters large and small. "At Riggs, we just don't harden our servers," Dixon explains, referring to the process of placing a dedicated security device at the service and application layer.

"We secure the desktops so that instant messaging, say, or non-authorized use of e-mail doesn't put the organization at risk for information leaks."

As Dixon alluded to in his comments above, a good security policy serves as one mechanism, along with the policies and practices of human resources, to control how business users behave when they use their laptops, desktops, and Blackberries, for instance.

Specifically, a well written, widely referred to, and well understood and enforced security policy can have the net effect of presiding over what the worker bees do, along with controlling content dispersal (one goal of all privacy regs).

And, getting users on board counts. Susan Fienberg, a senior analyst with TowerGroup, Needham, Mass., worked on a recent survey about authentication, and points out that policy and practice most conflict in the log in/authentication arena.

"Every security expert will tell you that the logging in process needs, say, complicated passwords to really make it do what it should. But users don't like complicated passwords—hence the conflict," she says.

And yet security policies are crucial because—in a complex, constantly shifting environment—these documents can do their bit to save the bank from fines, lawsuits, customer mistrust, and damage to reputation resulting from data leaks, denial of service, or other performance issues, notes Jack Danahy, president and CEO with Ounce Labs, Inc., a risk assessment firm based in Waltham, Mass.

"When you think about it, it's weird for use of applications and systems *not* to be defined and tracked the way, say, that bad debt is both defined and tracked," Danahy says, "and used to gauge overall business performance. Policy and standards can get something seemingly intangi-

## Dialogue

Continued from page 58

longer have value. A vital records approach takes that sort of organizational thinking a step further and encompasses the administrative aspect of records management. That is, the approach basically says, "these records have value for the following reasons."

Records then can get categorized and prioritized. Moreover, the firm can develop methods for searching them, making the records function more like a library for easy legal search, say, and less like a general repository that requires a lot of manual searching.

**Did last August's al-Qaida scare related to detailed surveillance of financial institutions shake things up?**

Yes. We were strongly reminded of the events of Sept. 11, and any complacency the industry might have had was shaken off. I believe that the catastrophic event risk for commercial banks is higher today than it's ever been, which is probably why demand is up for immediate disaster recovery and longer term backup systems.

The Fed has also put the pressure on financial institutions to enhance resiliency.

All of these systemic pressures mean that firms need to get organized with records, and protect what matters most.

**What other steps would you recommend?**

Right now businesses are functioning in the "Sarbanes-Oxley" era where there will probably be an over-reaction and a "micromanagement effect." Yet, as any long-time watcher of the industry will tell you, regs heat up and cool down in cycles. The bigger issue for a bank is, what is the resiliency profile, no matter what the regulators expect in a given period?

One key challenge that the industry faces is that it is so distributed in nature, both in terms of the vendors it works with in third-party arrangements and, on the corporate side, in terms of client interactions.

Different facets of the organization will have different storage requirements. For instance, what is the function of the document? Does it feed into a broader workflow system or is it a "standalone" item? What are the disaster recovery requirements given the type of record it is?

There are numerous DR options when it comes to records, including offsite, bi-location, central vaults, distributed storage. I would argue that the only reasonable way to begin making decisions is to know what you have overall, in terms of data, and to keep it all in a highly organized way—like a library—as a necessary first step. ***BJ***

## briefing

**ELDERS** *continued from page 14*

have opposed such legislative remedies.

### Maine: working with a state agency

Maine doesn't have an elder abuse law applicable to banks—only for the medical profession, according to Mark Walker, vice-president and council of the Maine Bankers Association. Several years ago, there was a proposal for such a law, which MBA opposed, and which was defeated. "We opposed it because evidence of financial abuse of elders is such a subjective observation," states Walker.

The Maine bankers did pledge, however, to work with the state's Bureau of Elder and Adult Services to offer training to bank employees about signs of abuse to look for and what protocol to follow. The association has also worked to have the state's banking code changed in regard to customer privacy to permit the reporting of suspected abuse. An employee can share the name of the elder customer with the bureau if the employee is making a good faith effort to report the problem.

The bureau, says Walker, is very good in its training efforts, and has various success stories it shares with bank employees.

### New York: considering the options

As previously mentioned, The City Council of New York's Committee on the Aging, chaired by Council Member Maria Báez, held a hearing to examine how to stop financial exploitation of seniors. Some of the suggestions put forth: amending New York State penal law, revising the statutes for obtaining power of attorney, reforming the Medicare/Medicaid laws so that seniors can keep their property while they receive their benefits, and the creation of Fiduciary Abuse Specialist Teams (FAST)—a team comprising financial experts from both the public and private sectors that specialize in financial abuse.

According to a statement distributed at the hearing, New York's larceny, identity theft, and unlawful possession of personal information statues don't criminalize the financial exploitation of an elderly or mentally incapacitated person. To prosecute these crimes, district attorneys have resorted to using other laws on the books. One of the district attorneys who testified cited the use of the hate crimes statute which lists age as a targeting factor.

At the federal level, the Elder Justice Act was introduced in last year's Congress. It was designed to protect the elderly from all kinds of abuse, neglect, and exploitation on the national level. The bill however, did not pass. According to a representative from the Committee for the Prevention of Elder Abuse, a version of the bill will be reintroduced in the 109th Congress. *BJ*