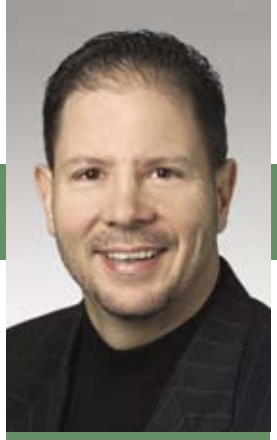
z/Bottom Line



ERIC L. VAUGHAN

Time to Be Cryptic

As the Information Revolution evolves, there has been an immense shift of responsibility in the custodianship of the critical and very personal information that resides on the world's IT platforms. With the onslaught of legislation over just the last five years, including HIPAA and Sarbanes-Oxley, CIOs now find themselves in the position of Chief Security Officer as well—with the potential of personal repercussions if their custody is mishandled.

IT organizations have naturally placed intensive focus and committed serious resources to plugging the "security holes," which include virus protection, SPAM, phish blocking, and hack attempts. Firewalls, Demilitarized Zones (DMZs), port blocking, IP filtering—it sounds like a full-out military operation behind the network walls!

But recent events reported in the press have highlighted a potential exposure that's about as small as Lance Armstrong's will to win. Iron Mountain, Inc., which was one of the first companies to introduce offsite data protection and tape vaulting services, recently "lost" some of its clients' tapes in transit. In May 2005, Time Warner, Inc. reported that names and social security numbers for 600,000 current and former employees were lost during Iron Mountain's pick-up and drop-off procedure. To add an element of intrigue to the event, "a source close to Iron Mountain said the truck was stolen when the driver stopped to get coffee." Iron Mountain denied this. On the heels of this revelation, Iron Mountain again made the news when it was reported in July 2005 that two backup tapes from Los Angeles-based City National Bank were lost during transport. These tapes contained account numbers and other customer information.

In both cases, the companies affected reported no fraud or misuse associated with the misplaced data. But beyond the potential for actual misuse, the political and business fallout can be substantial just from the occurrence of the events, due to media reports and notification procedures. In fact, under California's Security Breach Notification law, companies are required to provide notice of a breach in the security of data to any resident of California whose unencrypted personal information was, or is "reasonably believed to have been acquired by an unauthorized person." U.S. Federal legislation is pending along the same lines. One insurance-industry CIO who was compelled to write such a letter to a few customers recently told me that his new focus was to ensure he never had to write another.

This new wave of concern is all centered on one concept—one our industry should admittedly be very good at: being cryptic.

Encryption is the gateway to solving these issues. Suddenly, CIOs everywhere have discovered that nearly all their data lies resident on their disk and tape storage in unencrypted format, and is being carried out the door, put into trucks, and transported without the assurance of delivery. Iron Mountain's series of unfortunate events seem to be an aberration. They report they lost only four sets of customer backup tapes among the 5 million-plus trips they made this year. But if your tapes are in one of the four, the ratio won't matter.

Iron Mountain is also quick to say, "Given the criticality of disaster recovery and the need for privacy protection, we continue to recommend that companies encrypt backup tapes that contain personal information." But according to the Enterprise Strategy Group, only 7 percent of businesses encrypt all backup tapes. For this backup and offsite scenario, the paradigms need to shift. Many companies are looking at disk-based, offsite backup capabilities that use encrypted transmissions as a new method. One such company has the single most hilarious piece of marketing material I've ever seen: www.backuptrauma.com.

But a recent announcement of a new approach from Fundamental Software (www.funsoft.com) is of particular interest to the zSeries community. Known previously for their highly successful and incredibly capable Flex-ES mainframe emulation software, Fundamental recently announced their Flex-CUB (Control Unit Behavior) device. The Flex-CUB attaches via ESCON to your zSeries processor, and provides many capabilities, including emulating DASD, printers, and most important for this discussion, tape devices. So with two Flex-CUBs, one at your local data center and the other at your Disaster Recovery (DR) site, your backup "tapes" could be written to the local Flex-CUB in real-time. The local Flex-CUB can then transmit the encrypted files over a communication link to the DR Flex-CUB device. The benefits are obvious: a) no tapes are involved for the backups, b) the data is encrypted when stored, c) and then automatically transmitted in encrypted format to the DR site d) without waiting for a "vaulting company" to pick up the tapes, and e) your DR site is already prepared with your most valuable data without having to restore the files.

Protecting data in all forms is a pressing objective for all CIOs. And various approaches to encryption will sponsor a new wave of innovation as the vendor community responds to an emerging and pressing need. As Yoda would say—"Encrypt we must."

And that's &/=*J$^%J:p3.

About the Author

Eric L. Vaughan is president and CEO of illustro Systems International, LLC. He has more than 20 years of experience in the IT industry and is leading illustro in its focus on helping IT executives extend and enhance their existing investments.
Voice: 214-800-8900 • e-Mail: evaughan@illustro.com