z/Bottom Line

ERIC L. VAUGHAN

Inside Information

This column is about civic duty. Many industry analysts have ceded the conclusion that as a centralized data server, the mainframe continues to stand alone, guarding by some estimates up to 70 percent of the world's data. This is a staggering responsibility, and as citizens of the mainframe community, it's critical to self-preservation that we take this seriously.

"Yawn," you say. "We're doing everything possible to ensure the mainframe remains secure." It's true in most of the obvious ways. Literally billions are being spent annually to protect and safeguard not only the mainframe, but the very network infrastructure that surrounds it and provides a portal to would-be miscreants seeking to steal or destroy valuable information. We start with time-tested security software (e.g., IBM's RACF, CA-Top Secret, CA-Alert) that logs access, guards against unauthorized usage, and enforces corporate security policy. We harden our network with a variety of robust anti-spam and anti-virus tools to detect and shut down illegitimate attempts to use the system. We make enormous investments in equipment, software, and people for firewall and other intrusion-detection devices. We enforce Virtual Private Network (VPN) access for remote users. We have staunch policies and procedures for our distributed assets, including LAN and desktop virus protection and restricted configuration. We have plugged every hole in the dike.

Except perhaps for one, not-so-insignificant entrée to our vital repositories of information—the free pass given to all authorized users, whether employees, vendors, partners or customers, aka "insiders."

According to 2006 survey results from the Association of Certified Fraud Examiners (ACFE), every company in the U.S. loses an *average* of 6 percent of its revenues every year due to fraud. According to the survey, this fraud results in a loss of approximately $650 billion in terms of overall impact on the American economy each year. The ACFE also found that 60 percent of the fraud cases involved company employees, partners, vendors, or other insiders. The Federal Deposit Insurance Corp. (FDIC) published a report claiming that 65 to 70 percent of identity theft cases are committed with information stolen by insiders. Yet, most of the fraud is detected either by tips from someone else or by merely stumbling upon evidence by accident.

When provided with this information, people typically recoil in disbelief. "If it's that pervasive, why don't we hear more about this type of perpetration?" According to Ernst & Young, it's largely because companies don't want to publish such negative information, which could cause embarrassment, erosion of confidence, and loss of business. In the absence of legislation or regulation requiring such disclosures, you can almost guarantee these events will be handled as "an internal matter."

You may think that guarding against the systems and technical staff, or "super users" as they're sometimes referred to, is the call here. Not so fast. Research provided by Carnegie Mellon University in the banking and finance sector for the U.S. Secret Service dispels that myth. The research concluded that most fraud incidents required little technical sophistication. In 87 percent of the cases, the insiders employed simple, legitimate user commands. In 78 percent of the incidents, the insiders were authorized users with active computer accounts at the point of misappropriation. Contrary to preconceived notions, only 23 percent of the insiders were employed in technical positions. So these aren't hackers extraordinaire, but merely people with authorized access.

SOUND OFF!
Comment on this column by visiting http://community.zjournal.com/EricLVaughan.

Add the regulations and legislation, including Sarbanes-Oxley, Gramm-Leach Bliley Act (GLBA), and Health Insurance Portability and Accountability Act (HIPAA) to this daunting task of protecting and safeguarding data and the audacity of the responsibility comes into full view. These regulations not only mandate protection against misuse, but mere *access*, meaning we have to devise a way to detect if someone actually views data without proper authority, regardless of what they do with the data.

The good news is that awareness of the insider threat is improving, as is the technology to control it. Innovative technology exists that can, for example, record all 3270, 5250, Web and client/server data passing through a system and log that data to a searchable database. An IT professional, auditor, or fraud examiner could then use the system to search for improper usage or access, or better yet, to positively determine that it isn't occurring. This same technology can be set up to apply business rules to monitor for data access patterns and proactively issue alerts to appropriate personnel. Such technology provides other tangential benefits, but most important, it delivers a way to know who is accessing what and when, and provides the means to discover why. It's better to know.

Access to information has forever changed, and if we want to continue to hold the moniker as the safest place to centralize and serve data, the mainframe society must respond. All in favor say "aye." Opposed? If continued viability is the goal, the ayes have it.

And that's z/Bottom Line.

About the Author

Eric L. Vaughan is president and CEO of illustro Systems International, LLC. He has more than 25 years of experience in the IT industry, and is leading illustro Systems in its efforts to help IT management transform their mainframe investments. Comments and suggestions are welcome.

Email: evaughan@illustro.com; Website: www.illustro.com