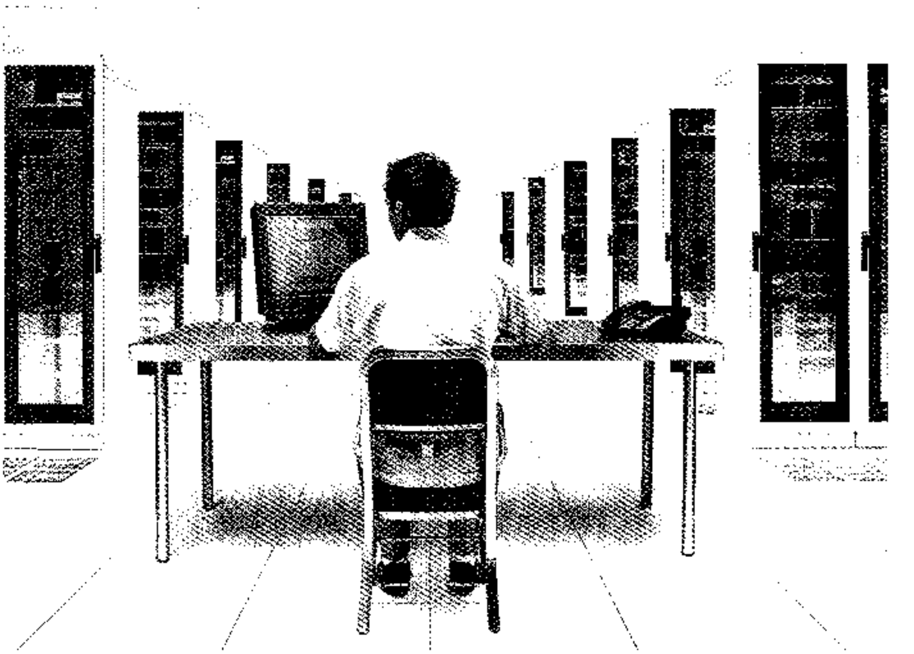
Do You Know Where Your Data Are?



The spectacular implosions of Enron, WorldCom, Global Crossing, and other tech companies several years ago continue to reverberate. Just last month the Sarbanes-Oxley Act of 2002, a law designed to regulate the accounting procedures of publicly traded U.S. companies and their non-U.S. operations, began going into effect. As information-technology departments scramble to accommodate the law's rigorous reporting provisions, they must rue the day they became the official cosmologists of a chaotic new electronic universe.

A backbone section of Sarbanes-Oxley requires a company's management to verify and swear that it has adequate "internal controls" to ensure reliable—accurate—financial reports. These internal controls are vaguely and broadly defined in the act, but they basically mean keeping exhaustive track of data related either directly or indirectly to the financial state of the company. To make sure their financial reports are accurate, companies must control and monitor all their reporting procedures and mechanisms, and also everything in the surrounding corporate environment that could affect the accuracy of their data. That environment includes e-mail and instant messaging, along with all documentation contained in everything from word processing tools and PowerPoint presentations to spreadsheets and custom-built databases.

This and other data-demanding legislation put IT at the center of a whole new information universe. To function in it, IT specialists will have to lean harder on such tools as data consolidation and integration, data storage and mining, and data documentation. Even chores like server cleaning and data backup will take on legal significance.

To comply fully with the Sarbanes-Oxley rules, companies are going to have to come up with extensive electronic communication policies. And those policies may mean that many of us—the Web-surfing, e-mail-sending, spam-attracting, online-bill-paying, Amazon-holiday-shopping, IM-chatting, MP3-downloading, security-breaching rank and file—will have to accept more intrusive oversight by IT. Though the rules apply only to public companies at the moment, it's quite possible they will soon extend to academic and other nonprofit organizations.

Strip away the thickets of regulatory jargon, and it becomes clear that companies are being required to have nothing less than a continuous, real-time, "God's-eye" view of everything in their corporate systems. They need to know exactly what to delete and what to keep. They must be able to monitor what all their colleagues and co-workers are doing online. And the personal and criminal liability for corporate officers who don't will be high.

Such problems may not seem daunting for a firm with 20 employees, but what if you've got tens of thousands or more? Where then does the Kuipers Belt of e-mail end and the Oort cloud of instant messages begin—10 trillion messages? 10 trillion million? Not even the late Carl Sagan could help us with this one.

Sarbanes-Oxley will probably benefit us all—better corporate governance and business practices will make viable tech companies less likely to be killed by corruption or greed, eliminating jobs and wiping out stock portfolios. But the more data we collect about ourselves [see "Managing Care Through the Air" in this issue], the more vigilant we have to be about how it can be used. Now that we are forcing companies to know a lot more about what their employees are doing, we must think through the social as well as the legal issues. As is so often the case with technology and regulatory developments, the challenges are not so much those of technology but of social responsibility and maturity. ■

YVETTA FEDOROVA
STEPHEN SWINTEK/GETTY IMAGES

The editorial content of *IEEE Spectrum* magazine does not represent official positions of the IEEE or its organizational units. Please address comments to Forum at n.hantman@ieee.org.