

Solved

THE PRIVACY PROBLEM FOR LEGAL DATA STORAGE

In a world of growing regulatory requirements surrounding data privacy, IT and business managers must safeguard the data in their care to the utmost of their ability. Here's how to ensure that data privacy is maintained in the data storage environment

Data privacy concerns have skyrocketed in recent years as companies become aware of just how vulnerable they are. The Privacy Rights Clearinghouse estimates that more than 94 million personal records were exposed in security breaches between February 2005 and now. And it's not just the Citibanks of the world that were affected.



Take the case of the Bisys Group, a New Jersey provider of investment and insurance solutions for financial firms. Personal details about 61,000 hedge fund investors—including the Social Security numbers of 35,000 individuals—were lost in June when an employee's truck carrying backup tapes was stolen.

The problem isn't confined to the financial industry. In early 2006, Providence Home Services, a Portland, Ore., provider of home health care services, reported that backup tapes containing Social Security numbers and some financial records for 365,000 customers were stolen. Other firms have lost tapes containing sensitive data when they were sent off-site for archiving and data recovery.

While this issue is troubling in its own right, it becomes particularly pressing in light of the slew of regulations that govern data privacy. Legislation such as HIPAA in the health care industry, Sarbanes-Oxley for publicly traded companies and Gramm-Leach-

Bliley in financial services all contain requirements that significantly affect how companies protect their data. The business consequences of not safeguarding corporate data rise with each new breach.

For midsize companies, there's an added element: They must comply with the same regulatory compliance mandates as large enterprises, but with fewer resources. Many find themselves scrambling to stretch an already strapped budget, or worse, having to take the calculated risk of not protecting information and hoping for the best.

This holds particularly true in the area of data storage and recovery. The business risk of noncompliance can be disastrous. One instance of noncompliance could cost a smaller company its business.

The Privacy Challenge

Traditionally, most companies have relied on tape, a technology that's been around for nearly a half century. While inexpensive, tape poses many security problems that could put business information at risk. It's slow and prone to error — tape backups that fail to record the data correctly are far from uncommon. Moreover, it's vulnerable to theft or loss during transport, and damaged, misplaced, lost or stolen

BY PROTECTING
THE PRIVACY OF
ATTORNEY-CLIENT
COMMUNICATIONS,
BOTH LAWYERS
AND THEIR
CLIENTS ARE FREED
TO BUILD THE BEST
POSSIBLE CASE.

cartridges can present a big problem if data recovery is required. Entrusting backup to employees unfamiliar with the process—or not interested in the task—is a recipe for error and neglect. Even storage vaults are not always safe.

In today's environment, the privacy stakes are even higher. No fewer than 31 states require companies to notify consumers when their unencrypted data is breached. This makes the case for online backup, which has always been compelling, even more attractive. And IT managers are catching on to the benefits of online backup. According to Gartner, 80 percent of businesses will be off of tape within the next 10 years. As IT managers look more closely at online backup, they should look for the following features to better protect and safeguard sensitive data:

- **Data Encryption:** Only the customer or data owner should have access.
- **When to Encrypt:** Data must be encrypted while it is stored on the storage array, as well as during transmission over private or public networks.
- **No Transmission Lag:** Data must be off-site or centralized as soon as the backup completes. Lags in transmission put the data at risk.
- **Central Management:** Look for the ability to centrally manage the backup and restore processes from one or more locations, ensuring that remote or branch office data is also reliably backed up and protected.
- **Managed Service:** A managed service strategy provides access to deep expertise and gives midsize companies access to enterprise-level protection without a huge investment.
- **Data Integrity Checks:** These must be done during transmission and once the data is stored.
- **Data Compression:** Allows for faster backup and recoverability.

Many companies have turned to online data backup as a faster and more reliable strategy. But as issues of data privacy become increasingly important, many are realizing that this choice is also a smart, secure method of protecting sensitive data. It could turn out to be a decision that pays big dividends. ■

legal

The attorney-client privilege is the cornerstone of the legal field. By protecting the privacy of attorney-client communications, both lawyers and their clients are freed to build the best possible case. In preparation for a case, law firms collect staggering amounts of data, much of it personal and confidential. That information then is stored in a database, and the database is regularly backed up and the data stored off-site. The repercussions of a data breach would be enormous, very possibly ruining a law firm's reputation and driving away clients.

In spite of this, most law firms use minimal security measures, although they are subject to the regulatory requirements of each client's industry as far as data protection goes. In fact, maintaining a certain level of IT security varies widely from firm to firm.

This problem is only exacerbated by the increasing use of electronic communications such as e-mail and file attachments. These documents must remain private, yet their presence online or in a company server renders them more vulnerable than if they were hard copy stored in a file cabinet. It would take just one successful breach in which data fell into the hands of opposing counsel or malicious hackers to bring a law firm to its knees.