

## In This Corner: Offsite backup is key strategy for compliance, security and cost-savings

Published: September 13, 2009

Font size: [A] [A] [A]



E-MAIL THIS



SHARE THIS

Everyone is feeling the pressure to lower overhead. The particular challenge for regulated industries like health care, banking, finance and insurance comes in making decisions that will not undermine quality and profitability.

Using health care as an example, decision makers have a strong operational and financial incentive to adopt electronic record platforms right now. The need to ensure 100 percent reliability, together with the initial investment and the obligation to meet security and compliance standards have tempered the pace of this transition for many small to midsized organizations.

For all organizations that collect and use personal and financial data, managing that data is a budgetary issue. Off-site backup, or what is now called "cloud storage," is an affordable, cost-saving technology designed to help regulated industries protect and manage data. Depending on what strategy an organization has in place, there can be tremendous gains in day-to-day operational efficiency and preparedness for routine audits - a welcomed reprieve for the people managing your IT network.

Using health care again as a model for all regulated industries, enterprise-caliber cloud storage achieves the first of five requirements of the Health Insurance Portability and Accountability Act Security Rule. The market is full of low-cost solutions that are ideal for the residential customer and sole proprietor. They fail to provide key business features. When evaluating a solution, it is advisable to focus on compliance, long-term storage capabilities and access controls.

Here are some specific guidelines to evaluate cloud storage services:

- Does the service provider offer systematic backup schedules to accommodate the need for continuous data protection?
- Does the archival component have the capacity to retain data for six years?
- Are there specified integrity and identity controls (repudiation technologies) to ensure files being stored are not altered and files in transit are not corrupted?
- Is the encryption technology FIPS-certified (government-grade) and will you control the encryption keys?
- Does the platform afford authentication and authorization controls?

Within most information-driven businesses, at least one person spends 15 percent of his or her time (more than one hour every day) managing backup and recovery. Tape and external drives have long been the local solution. Both are labor intensive, especially for organizations that receive and generate valuable, sensitive information throughout the day. Even when the person responsible for backup is beyond reproach, the limits of the hardware and the potential for computer and human error create liability.

It is important to note that transferring sensitive information to tape or to a backup drive also creates an unintentional security gap. Authentication and authorization controls - limiting who and what information people can access and change - are standard on most computer networks. These controls are generally lost with tape and drive backup procedures. Anyone who gains physical possession of the tape or drive gains full access, undermining the integrity of the system that the procedure is intended to protect.

The exponential growth in the volume of data is one last reason traditional approaches to backing up drain organizational resources. The need to upgrade or expand hardware capacity, replace tape libraries and find space to house archived files can be a significant burden. In a time when the value of every budget line and every strategy is under evaluation, automated and rigorously secure electronic backup provides an advance that also saves money.

MARC GONZALEZ is chief operating officer of Site 2, a Scranton technology firm providing disaster recovery and business continuity services to health care, financial, accounting, legal and governmental organizations.

IN THIS CORNER features commentary by guest columnists. If you would like to submit a guest column, contact Business Editor Jessica D. Matthews at [jmatthews@times-shamrock.com](mailto:jmatthews@times-shamrock.com).