Can Your District Survive a Data Disaster?

By Gary Smith

Imagine the impact of a data disaster in your district: payroll records and the entire accounting system are wiped out and the ability to submit mandated reports on time is not an option.

Although some school business administrators might think their district's current recovery plan is sufficient for "business as usual," if it fails, all financial records—including payroll—can disappear. That's why it is important to know without a doubt that essential business data can be recovered, how long recovery will take, and when normal operations can resume.

School business administrators have long recognized the need for a workable recovery plan regardless of cause. Yet many have not reassessed their current backup and recovery capabilities, perhaps because they have not experienced a catastrophic failure. Because their financial data may never have been disrupted, they may assume the current business data protection system is up to any challenge. Unfortunately, that may not be the case.

Holding your breath isn't an effective way to avoid a data disaster.

Three Serious Vulnerabilities

There are three reasons school business administrators may not realize or recognize that their recovery plans have, in fact, left them vulnerable to unacceptable long-term data disruption:

1. **Assumption that business data are safe:** School business administrators may be unaware of the various threats each system faces. In addition to hacking or even sabotage from former or current employees or students, threats include Internet viruses, equipment malfunctions, and natural disasters, such as tornadoes and floods.

   If the district's only backup solution is maintained at a site that is destroyed or compromised, the consequences and costs of business data recovery and the time needed to restore daily operations are nearly incalculable.

2. **Reliance on a tape backup system to retain and restore critical business data in the event of server malfunction:** Tapes have long been a staple and sometimes the only fallback for many school districts, but this old technology does not always work when needed. For example, backup tapes that record over a prolonged period are likely to wear out, causing data loss.

   School business administrators and their information technology personnel may not even realize that tape data have been lost until they try to access them, and that usually occurs when the servers that house the data have been jeopardized. By then, the damage has been done. For example, if the lost tape data include payroll records and if the servers, which are the beating heart of the data storage system, fail, the district could find it nearly impossible to recover personnel and financial information to ensure timely paychecks for employees and staff.

   Just ask Frank Ryan, director of finance for the Cobre Consolidated School District in Bayard, New Mexico. In October 2009, the district experienced a data disruption that threatened to wipe out all its data, including financial records. A cooling system failure in the room that housed 30 servers and the district's backup tape caused temperatures within to skyrocket to 120 degrees.

   Having the entire system in one room was nearly lethal for Cobre's most critical financial records. The heat was too much for all the equipment, including the backup tape mechanism, and the system started to fail. The district was on the verge of losing everything, including all financial and payroll data.

   "Fortunately this happened at midday while we were there. I don't want to think about all we could have lost had it happened at night," Ryan says, adding that he never considered the possibility of a heat-caused meltdown to the entire system.

Critical data backup requires a comprehensive data recovery and continuity plan.

   "The only way we were able to save everything was to initiate online emergency hosting through our business software vendor," Ryan explains. The emergency hosting consisted of quickly restoring an encrypted copy of Cobre's data to the vendor's data center via the Internet. "We were able to get our business operations running from their hosted data center within four hours," Ryan says.

3. **Failure to consider a recovery time objective in the data recovery plan:** It is important for any recovery plan to include a maximum window for data recovery and an operational system. For that reason, school business administrators should establish a recovery time objective (RTO): the deadline for recovering disrupted financial systems and other critical data without negatively affecting school business operations. Acceptable RTOs vary, depending on each school district's work environment and processes.

   The fundamental point is to maintain business continuity regardless of the nature of the disruption. For many districts, the RTO for critical data will be four hours to one day, and up to one week for noncritical systems. While these times are guidelines, school business administrators must determine whether different RTOs would be more in line with their data and business requirements.

   Another important consideration in RTO and recovery plan analysis is the level of support available from the district's business software vendor. School business administrators may need to reexamine whether the capabilities of the current products and the support contracts are sufficient should the worst-case scenario occur.

   Partnering with their business software vendor's support team to configure backups for quick recovery through emergency hosting and understanding the levels of support necessary for personnel to deal with data disasters are critical aspects of the district's data recovery plan.

The Hybrid Solution

One of the most important considerations in developing an effective data recovery plan is cost efficiency. School business administrators, always concerned about costs, can find their answer in a combination of the best of several options—a hybrid solution that ensures prompt data recovery without breaking the budget.

The hybrid's components for critical and noncritical data storage can include online backup, emergency hosting, disk-to-disk backups, and tape.

Why back up critical financial data off-site and preferably online? A private-sector survey about off-site recovery initiatives offers some answers that are readily applicable to school administrators. The Enterprise Strategy Group's April 2010 research report, *Data Protection Market Trends*, found that 42% of information technology professionals use an online backup service because of its "ability to store data remotely for disaster recovery." In addition, 30% prefer online recovery for its "predictable costs."

Critical data backup requires a comprehensive data recovery and continuity plan.

All the reasons cited in support of off-site and online data recovery deserve the same consideration for cost-conscious school business administrators. It is certainly more cost-efficient to have an off-site data center component as part of a hybrid solution that can also ensure security through encryption.

Reevaluating Data Recovery

In evaluating data recovery plans, it is important for school business administrators to begin with a business impact analysis that examines the three potential areas of vulnerability: safety and security of data, current backup, and an acceptable RTO for the district. Discussions with information technology personnel and the district's business software vendor can help steer the district toward the best solution.

Critical data backup requires a comprehensive data recovery and continuity plan that leaves nothing to chance and that is reviewed frequently. In the event of a data disruption, having such a plan is the only way to ensure that the district's business data can be recovered, that payroll can be processed, and that mandated reporting deadlines can be met. Consider it an affordable insurance policy against devastating data loss.

Gary Smith is vice president of sales and marketing for Windsor Management Group, based in Tempe, Arizona.