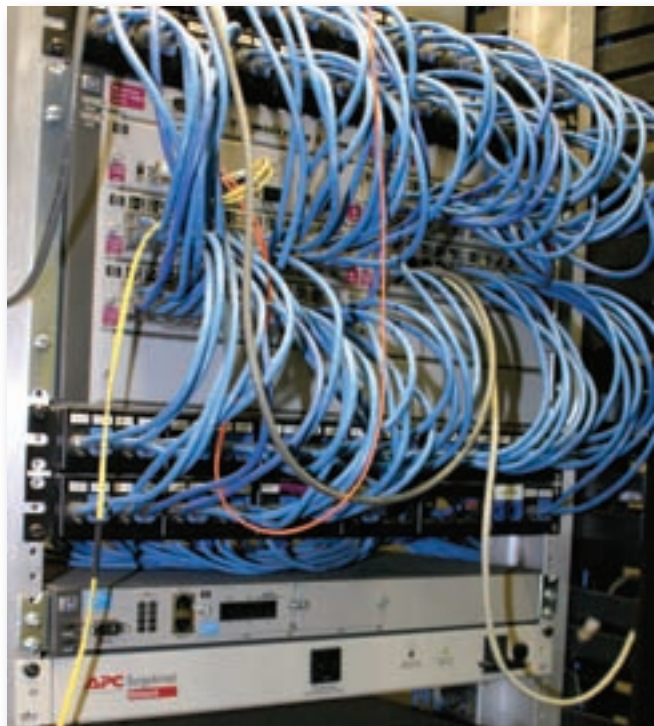


Protecting Schools' Electronic Data-Processing Systems

By Dennis McShane



Preserving records is important to schools. These records represent a lot of staff effort in developing grades, establishing budgets, documenting disciplinary decisions, establishing teaching plans, and communicating with guardians and the community.

Contingency planning is important to enable schools to “come back up to speed” following an unanticipated interruption or damage to the building, facilities, and data systems. Each school should identify those electronic records that are critical to continued operations, and those records that would be expensive or difficult to recreate. Once those records have been identified, the following risk-management techniques should be evaluated for applicability to your specific school.

- Important documents should be backed up electronically and moved off site on a regular basis. A few options for backing up data include
 - Having a duplicate server in another school building that automatically replicates the files on an ongoing or periodic basis.

- Making electronic copies on floppy disks, CDs, or tapes and carrying them off site for storage in another building, preferably in a fire-resistant safe or protected room.
- Backing up daily (the ideal frequency) but at least weekly. The frequency can be increased to daily during the end of the marking period or when teachers and administrators are busy updating budgets and grades.
- Electronic data processing centers should be protected by gaseous extinguishing systems (not wet sprinklers), and they should be located in areas that are subdivided and protected from the school’s other areas.
- Power surge protection for the building and for the specific computer equipment should be provided to reduce the chance of lightning or power surges damaging the sensitive electronic equipment.
- Contracts can be initiated with off-site electronic data warehouse companies that specialize in securing and protecting the backup data. Likewise, outside companies will offer contracts to provide temporary replacement systems while a damaged system is being rebuilt or replaced.
- The primary data systems within the school should be connected to an uninterrupted power supply, such as the emergency generator or a battery backup system.
- The server room should have adequate heating and cooling systems to maintain the temperatures within the manufacturer’s specified range. Temperature-monitoring alarms should be tied into a central station alarm service. Significant losses have occurred from overheated computer servers, and backup power to air-conditioning systems is recommended.

Other considerations include providing a secure site for storing laptops and related equipment and programs, as they are attractive items for theft, and ensuring that access to the systems is thoroughly evaluated for privacy and “need to know.” Staff should have secure passwords, and authorization to information should be restricted so that private information is accessible only to those who need it to perform their professional responsibilities.

Dennis McShane is a director of risk control for Glatfelter Public Practice. Email: dmcshane@glatfelters.com