

Search

THE Journal

March 2007 — News

Print this article

Data Security in K-12 School Districts

by Patricia Deubel, Ph.D.

Key words in data security are confidentiality, integrity, and availability. While K-12 school districts can address data security by putting systems and policies into place, I suspect that one additional issue is often overlooked. That is, data security is a people issue. Network administrators can't do it all. It takes knowledgeable and vigilant staff and students to support the process. One might categorize security at macro and micro levels.

Macro security: systems and policies

Data security threats can be intentional, unintentional, or environmental. When one thinks about threats to data security, hackers, remote access to the network by students and teachers, spam, and computer viruses quickly come to mind. Data can be lost or damaged in system crashes or when software programs in use freeze-up. Data might become corrupt due to faulty disks or disk drives. People might accidentally delete or overwrite data files. Data might be lost due to power failures, flooding, fires, bombs, tornadoes, or hurricanes. The list goes on. According to John Waters (2007), new security threats now include the use of Internet resources themselves, portable technologies (e.g., laptops, PDAs, USB devices, and memory sticks), phony e-mails, instant messaging, and peer to peer file sharing. At a macro level are the hardware/software and policies that districts put in place to minimize and contain those threats.

There are many products and services from which to choose.

Disaster Recovery. Security threats make districts more aware of ensuring plans for disaster recovery of financial, instructional, and accountability data. Districts can store data offsite using companies that provide back-up services for schools (Mills, 2006), such as Rediker Software or LiveVault. For day to day onsite recovery, Fortres Grand states that its Clean Slate will protect computers from malicious or inexperienced users by returning drives back to their original state upon reboot or log off. Thus, it protects original files from being modified and clears unwanted changes such as erased files, installed unauthorized software, downloaded spyware, adware, viruses, and Trojan horses, and any changes to icons. It also blocks unfamiliar executable files from running. Note also that Apple is building data recovery into the upcoming release of Mac OS X "Leopard" through a feature called Time Machine, which recovers not only at the file level, but also at the document content level.



Join education and technology leaders for an informative conference on data-driven decision-making!

**2007
TetraData
Leadership Forum**

*Leading the Quest:
Discovering the Treasures in
Your Students, Your Educators
and Your Data*

Sponsored by:

TETRA DATA
Software Company

Follett
Software Company

THE JOURNAL

April 24-26, 2007
Charleston Riverview Hotel
Charleston, SC

Conference seating is limited. For more information or to register, visit www.tetradata.com/leadershipforum or call 866-609-0783 x5569.

Malware protection. Firewall, anti-spyware, and virus protection software are needed, but such software tends to police access. Firewalls might actually inhibit what educators can do in the classroom by preventing access to appropriate internet resources and preventing them from downloading certain software they would like to try out (Waters, 2007). Anti-spyware like

- Next »
- 1. 1
 2. 2
 3. 3
 4. 4