EDTECH™ FOCUS ON K-12

Brought to you by:

CDW-G

CASE STUDIES

TACTICAL ADVICE

RESOURCES

Classroom

Infrastructure Optimization

Security

Storage

Networking

Mobile

Hardware & Software

Management

CURRENT ISSUE

Subscribe

Case Studies //

Protecting School Data with Endpoint Encryption

When data leaves school grounds, districts must address security concerns.

Karen D. Schwartz

posted August 16, 2012

Related Articles

Review: Symantec's Three-Pronged Approach to Data Security

How to Build a Secure Wireless Network

BYOD Lockdown Strategies

How to Keep Your Virtual-Learning Environment Secure

Schools Travel Different Roads to Cloud Security

Show and Tell

Features schools in: Nevada | Texas

Editors Picks

Security

With more than 300,000 students and 356 school sites, Nevada's Clark County School District is one of the largest

in the country. Such a large district produces a lot of sensitive data, about everything from grades to teacher evaluations.

For now, the district relies on its teachers and administrators to use good judgment, password protection and other security practices. Eventually, however, the technology staff hopes to increase protection by implementing endpoint encryption on the notebook computers its teachers and administrators often take home.

"Any time data moves from its native environment, it's at risk," says Lenore Hemphill, director for user support services. "We want to ensure that sensitive data is protected, whether it is at the school site, where we have procedures and technology in place, or on a mobile device."

But the move toward endpoint encryption will take some time, at least in Clark County. In addition to budget considerations, "we have work to do in transitioning our network infrastructure away from Novell toward Active Directory. Because of our size, it's complicated and time-consuming," says Chief Technology Officer Jhone Ebert.

Protecting sensitive data is one of the main reasons that organizations implement endpoint encryption, says Eric Ogren, CEO of the Ogren Group.

"If you're going to implement an endpoint encryption solution, look for a product that is transparent to the user, impossible for individual users to disable, and doesn't frustrate users who need quick access to data," he advises.

51%
The percentage of organizations that have lost data during the past 12 months as a result of the use of insecure mobile devices.

SOURCE: "Global Study on Mobility Risks" (Ponemon Institute, 2012)

Other school districts have found ways to attack the problem using different technological means. Technology decision-makers at the Austin Independent School District in Texas chose to bypass endpoint encryption, opting instead for a method that stores both data and applications in a secure private cloud. The school district last year implemented *Stoneware's webNetwork*, a unified cloud infrastructure that delivers all files and applications securely through a single user ID and password on any device.

"It's set up so all files accessed by administrators or teachers are saved to shared drives, which are behind our firewalls, secure and backed up, explains Jim Lax, AISD's information management support services director. "Users could circumvent the cloud and store drives locally, but they would have to go out of their way to do it, and we also have policies against it."

The method is also useful if devices are lost or stolen. If anything like that occurs, the IT staff can reimage a new unit with all of the user's settings within minutes, Lax says.

An Encryption Alternative

While the standard method of encrypting data stored on disks is to install an add-on product to do the job, another alternative is growing in popularity. Self-encrypting drives are designed to encrypt all data stored on a drive, within the disk drive controller. The user specifies a password, which is used to encrypt or decrypt the media encryption key. Encryption is transparent to users, who cannot turn it off.

"Self-encrypting drives have proved popular for primary storage of confidential data," says Eric Ogren of the Ogren Group. "With keys securely stored on the notebook, the IT department can manage the keys. That means

that IT can recover data if an employee leaves, or if the disk is archived for a long time."

Many hard drive manufacturers offer self-encrypting drives, including *Seagate*, *Micron*, *Fujitsu* and *Hitachi Data Systems*. Many notebook and desktop vendors also offer self-encrypting drives among their products, including HP's *Elite* and *Pro* lines of notebooks and desktops and Lenovo's *ThinkPad* line.

So why don't all school districts request self-encrypting technology? A self-encrypting drive can add a small amount to the price of a computer, and organizations often don't do a cost-benefit analysis to realize its worth.

"It's a strategic decision for IT," Ogren says. "It is easier to purchase a new device with self-encrypting drives than to retrofit already-deployed devices."

About the Author
Karen D. Schwartz
Karen D. Schwartz is a freelance technology writer based in the Washington, D.C., area.

Districts can get on the private cloud highway if they follow these key steps.

...more

Security

Product Review: Trend Micro Deep Security 8.0

New software lets IT shops manage security with ease in virtual environments.

What You May Not Know About Continuous Monitoring

It's essential to cybersecurity, but districts must establish an effective security...

...more

Storage

How to Find the Disaster Recovery Site Strategy that's Right for You

Consider the district's objectives and continuity needs before making an investment.

The Difference Between Aggregating Virtualization and Functional Virtualization

Not all virtualization technologies are created equal. Learn what differentiates these...

...more

Networking

How to Leverage the Power of a Protocol Analyzer

This troubleshooting tool is tops for diagnosing what ails the network.

More Tools to Consider for the 2012–2013 Back-to-School Shopping List

Here's a quick look at five cutting-edge technologies that can enliven classroom learning...

...more

Mobile

What Quad-Core Means for Tablets

The next generation of devices aims for faster video and app performance.

Rock-Solid: 3 Videos That Showcase the Virtues of the Panasonic Toughpad

Rugged tablets are living up to their name.

…more

Classroom

Infrastructure Optimization

Security

Storage

Networking

Mobile

Hardware & Software

Management