EDTECH™ FOCUS ON HIGHER EDUCATION

Brought to you by:

CDW·G

CASE STUDIES

TACTICAL ADVICE

RESOURCES

Classroom

Infrastructure Optimization

Security

Storage

Networking

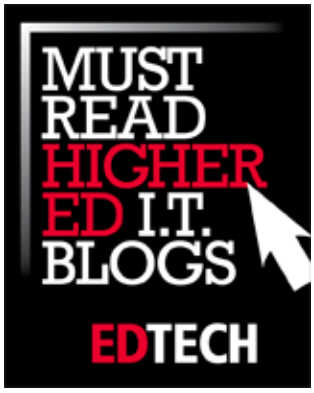
Mobile

Hardware & Software

Management

CURRENT ISSUE

Subscribe



Encryption

How Colleges Protect Mobile Data

Encryption software guards sensitive data when it goes on the move.

Karen D. Schwartz

posted August 16, 2012

Related Articles

Review: Symantec Endpoint Encryption Device Control, Full Disk Edition and Removable Storage Edition 8.2.2

Check Point Focuses on Endpoint Encryption

University of Louisville Takes Realistic Approach to Security

Five Security Tips to Lock Down Your BYOD Environment

Before You Click, Think Security

Editors Picks

Three Easy Steps to BYOD

5 Tips for Optimizing Load Balancers
Why Computer Labs Are Still Essential On Campus

Even a school dedicated to educating musicians has to take technology seriously these days. At the Eastman School of Music within the University of Rochester, students spend time learning while administrators and staff worry about safeguarding information.

“We are an urban environment several miles away from the rest of the university, and we have had plenty of thefts here — not only of notebooks, but of desktops,” says Jacob Cebula, associate director of computing services.

To protect sensitive data on Eastman-owned notebooks, the IT department needed comprehensive full-disk encryption software with a management console that would allow IT staff to monitor security. *Check Point’s Full Disk Encryption Software Blade* turned out to be the ideal composition. The first wave of implementation coincided with the deployment of a batch of notebooks this past summer. Next, the IT team will spend time retrofitting existing notebooks with the Check Point software. Cebula hopes that all notebooks used by staff and faculty will have the encryption software by 2013.

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.

Brown University’s IT department manages about 1,000 notebooks used by staff and faculty members. To help protect sensitive information, the university last year invested in *Symantec Endpoint Encryption*, which fully encrypts hard drives in notebooks. Chief Information Security Officer David Sherry expects the rollout to be complete by the end of this calendar year.

“We’re neighbors with Massachusetts and have a lot of colleagues who live there, so we wanted to comply with the Massachusetts data protection law,” Sherry says, referring to 2010 legislation that requires businesses to encrypt all personal data of Massachusetts residents. “The university has a very healthy regard for protection of data in motion, as well as regulatory action.”

The first phase, currently under way, is to retrofit high-risk notebooks — those with access to sensitive data. Once that is complete, the IT department will encourage staff and faculty, who may use personally owned notebooks, to have the software installed on their devices. Finally, new notebooks will be outfitted with Symantec Endpoint Protection before they are issued to users.

Sherry expects endpoint encryption will be needed for smartphones and tablets, as well. The university already issues tablets and smartphones to some employees, as well as allowing faculty and staff to bring their own devices. A mobile device working group at the university is developing a plan to protect data on those devices, Sherry says.

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

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 colleges and universities 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.

Classroom

Does Distance Learning Encourage Cheating? [Infographic]

Affordable access to online learning creates new opportunities for cheating.

Will Technology Push Colleges Away From the Traditional Lecture Model?

A new survey by CDW•G finds that students learn best when professors use a mix of…

…more

Infrastructure Optimization

Client Virtualization Saves Money and Improves Performance

Universities cut costs and run desktops more efficiently with client virtualization.

Trend Micro Deep Security 8.0

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

…more

Security

What Colleges Can Learn from Mat Honan's "Epic Hacking"

Simple security measures can prevent digital catastrophes.

Review: Symantec Endpoint Encryption Device Control, Full Disk Edition and Removable Storage Edition 8.2.2

Get control of your organization's data security policies.

…more

Storage

Colleges Use Storage Virtualization to Support Distance Learning

As colleges expand online learning, storage takes center stage — and virtualization makes…

5 Strategies for Deploying Deduplication Effectively

Deduplication can save space, time and money, but it must be done correctly.

…more

Networking

Increase in Devices Causing Bandwidth Trouble on Campus [Infographic]

How can IT departments keep up?

Dark Fiber Delivers for Columbia College Chicago

An upgraded network at the noted arts and film college gives students and faculty the…

…more

Mobile

Call Me, Maybe? The College Student's Affair with Smartphones [Infographic]

How are students using their high-tech smartphones?

3 Ideas to Make the Most of Mobile Apps on Campus

Students already have the devices, so how can schools embrace the trend?

…more

Classroom

Infrastructure Optimization

Security

Storage

Networking

Mobile

Hardware & Software

Management