STATETECH Technology Insights for Leaders in State & Local Government

CASE STUDIES

TACTICAL ADVICE

RESOURCES

Infrastructure Optimization

Security

Storage

Networking

Mobile

Hardware & Software

Management

CURRENT ISSUE

Subscribe

Home » Security

next ›

Encryption »

Sensitive Data Demands Protection

States deploy encryption software to safeguard mobile devices.

Karen D. Schwartz

posted August 17, 2012

Related Articles

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

Five Security Tips to Lock Down Your BYOD Environment

Serving Up Anytime, Anywhere Apps Over a Private Cloud

Review: Symantec Endpoint Protection.cloud

Governments Take Different Paths to Cloud Security

Editors Picks

How Governments Save On IT By Joining Forces

5 Tips for Optimizing Load Balancers

The Rise of Machine-To-Machine Communications

4 Ways Surveillance Cameras Become A Necessity For Safety

State by State

In this article: Indiana

With a mission as sensitive as protecting children, it makes sense that New York's Office of Children and Family Services has adopted mobile data encryption software.

"We understand that encrypting our data at rest is not only a best practice but a requirement, given the potential risk," says William Travis Jr., CIO of the OCFS. "For citizens to call in to report a child abuse allegation, they have to have confidence that we are safeguarding their information."

Each of the approximately 5,000 notebooks used by the agency's child protective investigators, foster care workers and child care facility inspectors is outfitted with *McAfee Endpoint Protection*, which encrypts data on the hard drives. The department standardized on McAfee in 2010 as part of an enterprise mobility effort.

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.

Indiana has enforced full-disk encryption on its nearly 10,000 state-issued notebooks and tablets since about 2007. The reason, says Paul Baltzell, deputy CIO for delivery services, is to ensure that sensitive data is protected even when employees take units home or on business travel.

"We felt it was safest to encrypt everything across the board of the executive branch to protect all sensitive information," Baltzell says.

The state's IT department loads McAfee Endpoint Protection onto units before distributing them to employees. When the program is loaded, the software essentially takes over the boot sector of the drive, so when it boots up, users must authenticate to McAfee as well as to Windows.

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)

Although the full-disk encryption has been a success, it can take a toll on the speed of the machines. To remedy the issue, new units have Intel Core i5 processors, which have encryption instructions directly on the chip.

As mobile devices become more popular, Baltzell is taking a look at encryption on smartphones and tablets. He is

evaluating products from several vendors, including *MobileIron*, *Absolute Software* and *McAfee*.

OCFS' Travis also is looking at smartphone and tablet encryption. The office already has begun issuing Apple iPads to some of its employees and also is in the process of implementing a bring your own device (BYOD) strategy that will allow employees to use their own smartphones and tablets on the job. Every iOS device has a dedicated AES-256 crypto engine built between the flash storage and main system memory, which improves the efficiency of encryption on the device. Users who work with their own smartphones and tablets can access applications and e-mail via a secure URL, work directly in the application, and will not be able to store work data on their devices.

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 agencies 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 Schwartz is a freelance technology writer based in the Washington, D.C. area.

Infrastructure Optimization

Pull the Plug on Excessive Data Center Costs

IT managers find that they can take advantage of new technologies and techniques to...

Windows Server 2012: A Foundation for the Cloud

Migrating your organization's IT infrastructure to a private cloud? Windows Server...

...more

Security

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.

Sensitive Data Demands Protection

States deploy encryption software to safeguard mobile devices.

...more

Storage

Which Disaster Recovery Site Strategy Is Right for You?

Be sure to factor in the organization's objectives and continuity needs before...

The Difference Between Aggregating Virtualization and Functional Virtualization

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

...more

Networking

How to Make a Smooth Switch to IPv6

Determine business needs and evaluate existing environments before jumping into the new...

4 Awesome Google Fiber Videos

Kansas City is getting star treatment from the search empire.

…more

Mobile

What's Eating Up Your Data Plan? [Infographic]

Educate your employees about the complexities of mobile data plans.

Three Tips to Secure Telework

Follow this advice to protect data while working remotely.

…more

Hardware & Software

Ergonomics: The Health Intervention Your Organization Needs

More organizations focus on ergonomics to improve staff health, efficiency and the bottom…

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

Infrastructure Optimization

Security

Storage

Networking

Mobile

Hardware & Software

Management