5 Next-Level Data Consolidation Tips

Follow these five data management tips for a successful consolidation project.

next ›

Encryption»

How Agencies Keep Mobile Data Safe

Encryption technology protects data on notebooks and other mobile devices.

Karen D. Schwartz

posted August 20, 2012

Related Articles
Review: Symantec Endpoint Encryption Device Control, Full Disk Edition and Removable Storage Edition 8.2.2
How to Build a Secure Wireless Network
Serving Up Anytime, Anywhere Apps Over a Private Cloud
Review: Symantec Endpoint Protection.cloud
Policies, Not Tools, Drive Cloud Security
Editors Picks

How Adopting Shared Services Boosts Efficiency
Software for Monitoring and Management
Next-Generation Tech Gets Agencies Ready for Enterprise

When news broke that a Veterans Affairs Department notebook computer and external hard drive that included personal information for more than 26 million veterans were stolen in 2006, many federal agencies sat up and took notice. A month later, the Office of Management and Budget issued stringent new security policies that included a mandate to encrypt all data on notebook or handheld computers unless the data was classified as nonsensitive by agency leaders.

That mandate pushed the Census Bureau, like many other agencies, to adopt full-disk data encryption standards for its notebook computers. By early 2007, every Census agency notebook issued to employees was equipped with full-disk encryption. Today, that's 960 notebooks for headquarters staff and more than 6,000 for field employees and teleworkers.

"Our field reps conducting surveys around the United States have to comply with Title 13, which protects citizens' and businesses' private information, and our administrative staff and teleworkers always have to be careful about personally identifiable information," explains Mark Markovic, assistant division chief for customer support in the Census Bureau's LAN Technology Support Office.

To access their hard drives, employees enter a user ID and password; the hard drive stays encrypted. The Census Bureau also has policies in place to regulate what information may be downloaded or removed from the hard drive.

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.

Officials at the Federal Deposit Insurance Corp. were similarly affected by the mandates that came out after the data breach at Veterans Affairs. Russell Pittman, CIO and chief privacy officer of the FDIC, first tried file-based encryption in an effort to avoid problems with employees attempting to remotely access their computers from home.

"We were trying to avoid full hard-drive encryption, because if they turn off their notebook before leaving work or it is rebooted, they can't access it and work remotely," Pittman says.

After using the file-based encryption for about six months, however, it became clear that it wasn't protecting data adequately. Instead of depositing files in an encrypted folder, employees testing the file-based encryption would sometimes inadvertently save data on a desktop or make a new, unencrypted folder.

Because security trumps convenience, the agency moved to full-disk encryption. Today, every one of the approximately 12,000 notebooks used by agency employees must comply with a policy to automatically encrypt the hard drive using the FIPS 140-2 algorithm.

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)

"Unlike file encryption, where people could get to the hard drive and try to run things against the encrypted partition, nobody can access the hard drive without the right credentials when you're using full-disk encryption," Pittman says.

As for the Census Bureau, a plan is already under way that may relegate full-disk encryption to the back burner. The agency is in the midst of a virtual desktop infrastructure implementation, which will allow employees using any computing device to access files and applications from a private cloud, while prohibiting them from storing data to those devices.

"We're rolling it out to field personnel now, and it's also our solution for teleworking," Markovic 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 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."

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's Cloud Connection

Microsoft's newest server solution can help agencies migrate their IT infrastructure...

more »

Security

FedBytes: Is Communication the Best Defense Against Cyberthreats?

Hardware, software and tech news from across the government and around the country.

How Agencies Keep Mobile Data Safe

Encryption technology protects data on notebooks and other mobile devices.

more »

Storage

Which Disaster Recovery Site Strategy Is Right for You?

Be sure to factor in the agency's objectives and continuity needs before making an...

NAS Creates Lots of Storage in a Small Space

Network-attached storage devices can fulfill the needs of both large and small...

more »

Networking

New 802.11ac Wireless Standard Promises Gigabit Speeds

With more traffic going wireless, agencies can look to the next Wi-Fi standard for...

How to Make a Smooth Switch to IPv6

Determine agency needs and existing environments before jumping into the new...

more »

Mobile & Wireless

New 802.11ac Wireless Standard Promises Gigabit Speeds

With more traffic going wireless, agencies can look to the next Wi-Fi standard for...

3 Ways the Military Is Using Mobile Applications

How technology is powering the Army, Air Force and Veterans Affairs.

more »

Hardware & Software

Maximizing Windows 8 Security Features

Three core enhancements can improve 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.

more »

Infrastructure Optimization

Security

Storage

Networking

Mobile & Wireless

Hardware & Software

Management