At Rest — On Guard

If you want to let data idle, make sure you have protections in place to secure those files at rest.

By Karen D. Schwartz

Photo: Randall Scott

You get the most bang for the buck by locking down user-access privileges and requiring users to authenticate with two factors, National Defense University's John Rossi says.

It happened again: government records exposed because of a notebook computer theft.

The most recent breach — a notebook containing 2,500 patient records nabbed from a researcher's car on the National Institutes of Health campus — is just the latest in a string of high-profile incidents. Although the NIH notebook was password-protected, the personally identifiable information wasn't encrypted.

Securing data at rest, a top federal priority, remains complex. The number and type of encryption algorithms are confounding, the security technology is still maturing, and policies are still evolving. Even so, say several experts, protecting data at rest should not be dismissed as an insurmountable challenge.

Layer by Layer

The ultimate solution involves several steps: knowing what you have, knowing what's vulnerable, classifying your data, keeping track of your devices, determining how best to encrypt your data and hardware, and assigning appropriate privileges.

But it's the combination of actions that's the crucial factor, says John Rossi, professor of systems management and information assurance at the National Defense University (NDU).

View each step as another layer of security, say Rossi and other security experts, making penetration and data tampering by would-be attackers more difficult and time-consuming to perpetrate. Here are their pointers on how to succeed at protecting data at rest, step by step:

Start with the basics. Multifaceted security technologies can go a long way toward protecting data at rest. But before diving in, do some basic blocking and tackling, says David Hollis, program manager and co-chairman of the Defense Department Data at Rest Tiger Team. DARTT manages blanket purchase agreements for data-at-rest encryption products.

Essentially, inventory your systems and identify your vulnerabilities, and then take them on one at a time, he says. "Some agencies haven't even started encrypting their mobile devices, and that's key because the environment is becoming more and more mobile."

Adds DARTT Technical Director Robby Carter: "It's about taking care of what we can, based on what's most vulnerable today, while the government determines resources and funding and technologies to support the infrastructure."

Inventory your data. Before you even think about securing data at rest, you have to know where it resides. "It's not as easy as it sounds because data is everywhere, and you really have to rely on the people who own the data to help identify where it is. And then you have to consolidate it and map where it's going — all before you can adequately secure it," says Patrick Howard, chief information security officer at the Nuclear Regulatory Commission and former CISO for the Housing and Urban Development Department.

Keep track of your devices. The ability to copy or move sensitive data onto small portable devices has increased vulnerability dramatically. One way to conquer that issue is through device discovery. Often provided free with security systems, device-discovery applications let users assess and determine what types of devices are

connecting to the network. The information provided by each assessment hinges on the particular user's administrative authority.

"That way, they have the information they need to determine the data leakage threat in their organization," says Dave Vergara, product marketing director for data security at Check Point Software Technologies. "If a lot of employees are copying business data to personal USB thumb drives or other removable media, including some things maybe they shouldn't be taking with them, you'll know that, and can then determine how best to take back control of it."

Classify your data. If you haven't set up a classification system for data based on its importance, sensitivity and value, it will be impossible to ensure that new data is properly protected. "For example, if a certain type of data is classified as secret, it should be assigned this classification no matter if it's at rest or in motion; and anything created within these content parameters should be classified as secret," explains John Bordwine, senior director of security engineering at McAfee.

Encrypt your data. The pinnacle for data protection is confidentiality, integrity and availability to those authorized to access the data. A conflict, however, arises between confidentiality and availability — the more stringently data is protected, the more difficult it is to access, even by authorized users. And passwords simply don't cut it; they are reasonably easy to decipher, hard to remember and, in the case of the Defense Department, must change every three months and can't match any of the previous 24 passwords that you've used.

fact: 159 million: Records containing personal and private information breached in the United States since 2005
SOURCE: Spyrus

"There are many problems with passwords in general," says NDU's Rossi. "You can hash them, but if you lose the keys you won't be able to unlock it. And because passwords have to change so often, they become almost impossible to remember."

So what's the solution? Use a combination of something you know (a password), something you have (a smart card or token) and something you are (a biometric). "If we did just that, we would be 80 percent there," he says.

For portable hardware, media encryption and port protection make sense. The technology, which combines port and device management, content filtering and centralized auditing with media encryption, plugs potential leads and logs data movement to and from devices. "If the device isn't approved, it won't allow the user to write data to it. If it is an approved device, policy settings can ensure that the data is protected by forcing encryption of the data when it's copied to the device," Vergara says.

Be picky about privileges. Try to limit access to those who really need it, and if granted, employ the concept of "least privilege" by authorizing the fewest number of privileges to accomplish essential tasks.

Segregate, whenever possible and practical, critical information system components, and limit network access to secondary storage devices containing highly sensitive information.

"It's about having a well-designed systems architecture and implementing a defense-in-depth protection strategy," says Ron Ross, FISMA Implementation Project leader at the National Institute of Standards and Technology. "If you do it that way and your system is breached, the attacker's access can be significantly limited."

Want more security suggestions? Read the Best Practice on the Federal Desktop Core Configuration.

The ABCs of Encryption

There are two basic types of encryption, and a third that is a hybrid of the first two.

Full-Disk Encryption (FDE), also called whole-disk encryption, is a process by which the entire contents of a disk is encrypted. It's a comprehensive system that works well and protects an organization against risk, says John Bordwine, senior director of security engineering for McAfee.

"Some organizations might decide only to encrypt things they classify as very sensitive information, but there might be some confidential information somewhere nearby," Bordwine says. "So if you encrypt everything on the hard disk, you get pretty close to ensuring 100 percent protection."

FDE isn't foolproof. It doesn't provide protection against online attacks, and integrity protection requires a strong hash function and a digital signature. What's more, performance can be adversely affected.

File Encryption Solution (FES) is the other end of the spectrum. This method, which involves encrypting individual files or directories, lets users back up files to other locations, such as USB thumb drives or e-mail messages, with the encryption still intact.

If you choose FES, make sure you have ironclad key management, because the file encryption key must be shared among multiple users. The best file encryption products hash and digitally sign both the plain text and the cipher text to provide nonrepudiation and prevent chosen cipher-text attacks.

Hybrid, or integrated FDE/FES, combines both approaches by encrypting the contents of a hard drive while retaining the ability to encrypt individual files or folders for data at rest.

"It allows you to selectively set up classifications for content, adding classifications for when new content comes into the environment," Bordwine says. "And even if you forget something, like to encrypt a particular hard drive or set parameters on a specific file server, you'll still catch it because you've got classifications set up."

DATA AT REST, IN THE REGS

- **OMB M06-16: Protection of Sensitive Agency Information — June 2006** Recommends encrypting all data on mobile devices, using two-factor authentication, and logging all computer-readable data extracts from databases holding sensitive information
- **Defense Department Guidance on Protecting Personally Identifiable Information — August 2006** Requires encrypting all data at rest - "all hard drives or other storage media within the device as well as all removable media"
- **Policy Memorandum: Acquisition of DAR Technologies For Use Within the DOD — March 2007** Provides guidance for enterprisewide acquisition of data-at-rest encryption technologies in the department and establishes the DOD Data at Rest Tiger Team
- **Policy Memorandum: Encryption of DAR on Mobile Computing and Removable Storage Devices for DOD — July 2007** Establishes DOD encryption requirements for data at rest
- **NIST Special Publication 800-53A: Draft Guide for Assessing the Security Controls in Federal Information Systems — December 2007** Designed to help develop consistent security controls

REST OF THE BEST

- Don't forget to encrypt backup tapes. It's expensive, but spend the money necessary to encrypt them because that figure will likely pale in comparison to the cost of recovering from a breach.
- Ditto for CDs. Some agencies encourage users to use WinZip's encryption for individual files saved to CD. Better yet, use encrypted thumb drives because they automatically encrypt data saved to them.
- Make your effort commensurate with the importance of the information to the organization. "The more critical that information is, the harder you should work to protect it and the more safeguards and countermeasures you should put in place," NIST's Ron Ross says.