Spring Cleaning

By Kevin Ferguson

Before you take a summer break, get your IT shop in order.

AS APRIL SHOWERS give way to May flowers, Elias Montoya's thoughts turn to spring cleaning. But you won't find a mop, broom or feather-duster in his hand; you'll find a keyboard and a mouse. For Montoya, director of information technology at Miami-based law firm Abadin Cook, spring cleaning includes performing a recovery to test the law firm's tape backups. "We have to verify that data once it's on tape," he says. "It's time-consuming, but worth it."

In truth, Montoya performs some chores on his spring-cleaning list perennially. He cleans the tape heads on the law firm's backup drives once a month. All servers get backed up nightly to an onsite network-attached storage device, and on a weekly and monthly basis, he turns to tape to store backups offsite.

DON'T LET PERMISSIONS SLIP

If your business has high employee turnover, or if you have an unending parade of contractors roaming the company network, now is a great time to review just who has been given access to which data and applications. Chances are that everything is fine — but do you want to leave it to chance?

Rich Haig, MIS director of New York City outerwear manufacturer Herman Kay, does not. "Everything we do is on a shared drive, so I need to make sure that the permissions are set properly, whether it's given to an individual or a group," he says.

In addition to the 200 people Herman Kay employs, the company works with many outside designers and photographers who are protective of their work. "I won't, for example, let my salespeople write over line art or recolorize something from the specified colors. That's the responsibility of the designer."

And that's the work of network-management software. There are many choices available, from Citrix System's Access Essentials, which includes access control as part of its remote desktop virtualization software, to Hewlett-Packard's ProCurve Identity Driven Manager, which grants or denies access based on a variety of factors, including the time and the user's location when access is requested.

Give yourself permission to protect your company.

"Tapes are not as reliable as backing up on a hard disk or other methods, because they tend to fail over time," Montoya explains, which is why he tests the backup system twice a year.

"It's not always a matter of the time of year, but that you are looking at something at least once or twice a year," says Rich Haig, MIS director at Herman Kay, a New York City outerwear manufacturer that employs 200 workers.

"We're selling wool outerwear to major retailers. We can't afford to print labels and ship the boxes only to find that they won't scan and the boxes get returned," Haig says. So every quarter, he checks the printers in the warehouse to make sure the labels they print can be scanned correctly.

Scheduled IT maintenance, whenever it takes place, is what matters, say Montoya, Haig and other small-business sachems. Among the tasks common to their to-do lists:

Conduct a full IT audit. Such an audit includes a full accounting of hardware, software, contracts and other IT assets. It should also include the mapping of directories so that the IT department knows where to find its files, software utilities and applications. Many small companies allow their workers

BRIAN SMITH

Elias Montoya tests law firm Abadin Cook's backup systems twice a year.

to download utilities, add applications and keep files on individual storage devices, such as thumb drives. But no central record of their existence is kept.

"Part of your audit should include creating or verifying an inventory of all your critical business software and applications," says Ross Oliver, owner of IT consulting firm Tech Mavens of Sunnyvale, Calif. "The inventory should include install and recovery media, internal personnel contacts, vendor contacts and maintenance contract information. The worst time to discover a maintenance contract is expired is when you need the maintenance."

Conducting an IT audit also makes good legal sense. Many businesses have unlicensed copies of software on their hard drives, quite often unwittingly. But that's still illegal. According to the Software & Information Industry Association (SIIA) in Washington, D.C., it amounts to software piracy and is punishable by fines and imprisonment.

Piracy aside, you don't want to overspend. Often, individual departments will buy new copies of expensive software applications, not realizing their company already has a volume-purchasing agreement. An easy way to tackle that problem is to use asset-management utilities, such as Novell's Zenworks Asset Management, LanDesk Software's LanDesk Asset Manager or Ipswitch's WhatsUp.

Update your IP address and network map. If you don't already have one, now's the time to break out an Excel spreadsheet or Visio chart and create it.

Centralized data stores make document retrievals easier and backups faster, says Stihl's Robert Hulings.

KEITH LANPHER

With a good map, "if you need to locate a workstation, you can look and see to whom that workstation is assigned, where it's physically located and what IP is assigned to it," explains Abadin Cook's Montoya.

Because it's based in Miami, Montoya's law firm is particularly cautious about restoring its systems in the event of a natural disaster. "If you have to re-create your network due to a catastrophe, then you will have a layout of your network," says Montoya. "It gives you a blueprint of what the network looks like so that you can re-create it without reinventing the wheel."

Montoya turns to his network map regularly when conducting Internet usage reports, analyzing server problems and adding new devices to the network.

"Everyone should have an IP list or layout," he suggests. "You don't want to assign the same IP address to two devices because they will conflict with each other. For example, if two PCs or any other two network components, such as a managed network switch or network scanner, have the same IP on the network, then the system will kick them off."

Centralize data stores. If your organization hasn't gone down the path of providing centralized, shared folders on file servers, now is the time. Power-tool maker Stihl Inc. recently completed a project to centralize file and e-mail data storage, including documents scanned from printers into e-mail, says Robert Hulings, LAN/WAN administrator for the Virginia Beach, Va., manufacturer.

By using Symantec's Enterprise Vault, Hulings created a single data archive that supports a number of source applications, such as Exchange. The archive keeps compressed flat files of documents available for a set period in accordance to company policy and automatically moves e-mail from user inboxes to archive folders to free up storage space.

"The local system drives do not get backed up at all," Hulings says. "We provide storage to departments and users, so documents must be stored on the server. We have it set up so that machines do not see the local hard drive, only the shared drives." With about 6 gigabytes of shared storage space per user, Hulings says there's no reason for users to want to back up documents to the C: drives.

Through policies set up in the company's storage system, Hulings can ensure that users don't store executable files and can retain certain types of documents—such as attachments or documents for different departments—for different time periods. Additionally, centralized stores ensure that IT can retrieve documents when needed and can back up its data stores faster.

Wait, back up. Don't assume your backup equipment is functioning properly. Run a test. There's nothing worse than thinking you're backing up your data, only to find out you're not. Also, back up everything before you purge old files from directories. "Many people make the mistake of waiting until after cleaning to run backups, so the backups will also be clean," says Tech Maven's Oliver. "The result is often both the systems and the backups are broken."

The latest backup software utilities — such as Symantec's Backup Exec 11d for Windows Servers and IBM Tivoli's Continuous Data Protection — back up data continuously, so you're covered up to the minute. That takes some of the planning out of the equation. The same holds true for products such as NovaStor's NovaNet-Web software, which lets IT administrators set up an Internet-based, automated backup for multiple users.

Toss out junk. Businesses collect a lot of software rubbish that clutters hard drives and wastes processing power. Temporary directories, particularly in Windows, are often the repositories of hundreds or even thousands of executable files left over from downloaded applications. It's time to haul this garbage to the cyber-curb.

Most of the companies that faced legal action for software piracy last year were small and midsize businesses with an average of 150 employees and sales of $17 million.
SOURCE: SIIA

"I have had a number of issues with disk space over the years where, as our available disk space dwindled, I lost time attempting to determine why our e-mail was not working when the problem was actually due to available disk space," says Tracy Pierce, chief financial officer of Precision Concrete Construction, an Alpharetta, Ga.-based company that employs more than 500 workers and builds corporate office parks, high-end residences and other structures across the Southeast.

Jon Czerwinski, vice president of Cohn Consulting in Marietta, Ga., agrees. "Space problems can manifest themselves in a number of ways that can be difficult to recognize immediately. Keeping abreast of the need for disk space is a simple step that can prevent many headaches," he says. "We recommend a company use policies and automation to clean up storage through mail-server archiving, removal of temporary files upon logon and logoff, and continuous defragmentation. This ensures the systems are always performing optimally."

A good place to start is the operating system registry. The registry is used to store information necessary to configure the system. In Windows, for example, Windows Registry contains information that Windows continually references, such as user profiles and the applications installed on the computer. Each time a user installs, removes or changes a program, the registry is updated and cluttered further, often with spyware, adware and other junk. That slows system performance and can lead to crashes. "That's why, if you use shared drives, as we do, it's important to clean out file directories for all users," says Herman Kay's Haig.

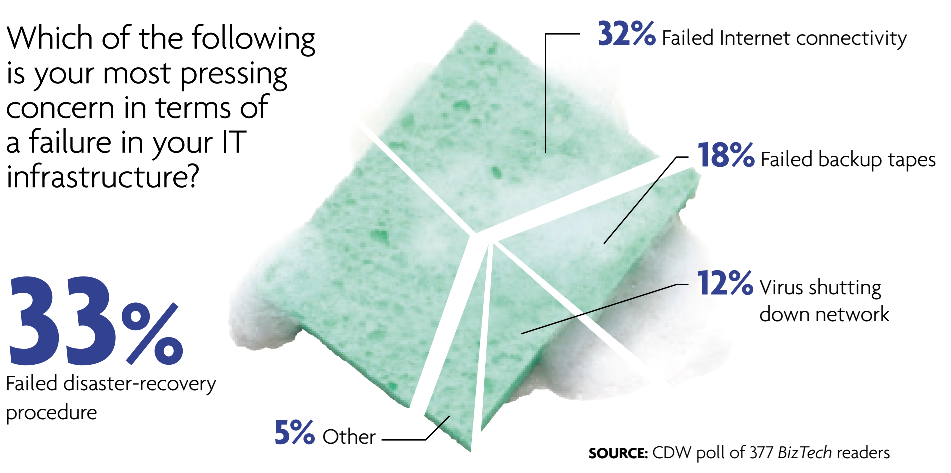
Stay safe. Fewer things are easier — and more costly to overlook — than making sure your IT security is up to date. Software licenses encourage users to sign up for automatic updates and patches. But how easy it is to click the "update later" option in the pop-up window — and that's just for your machine. How many other devices have been added to the network since you bought your license? Are all the devices up to date? Are they all in compliance with your company's security rules?

You won't know until you either manually check each program or automate software compliance policies. A company should ensure that operating systems and security software — antivirus, antispyware and antispam — have current updates, patches and definitions, advises Stihl's Hulings. "Security is a high priority right now with [the threats] from hackers and malware," he explains. "We constantly monitor for intrusion sweeps and spoofs, and we always keep our virus protection and scans up to date."

To further reduce risk, the SANS Institute, an IT security cooperative in Bethesda, Md., that works closely with the FBI, strongly recommends that IT administrators use automation to keep users from installing or uninstalling software and to make sure systems are fully patched. [BT]

QuickPoll

Which of the following is your most pressing concern in terms of a failure in your IT infrastructure?



SOURCE: CDW poll of 377 *BizTech* readers