

Information Technology: Put Your Computer Systems on a Regular Maintenance Schedule

By Jeremy Cherny, President, Tobin Solutions Inc.

It's likely that the owner's manual for your automobile includes a comprehensive guide to maintenance. Chapters are devoted to explaining how to monitor and check the various gauges and fluid levels. The manual probably includes a very clear schedule laying out a detailed plan for regularly changing your oil, getting tune-ups, and more. The auto makers provide these recommendations to keep your car running smoothly and reliably.

What are the maintenance guidelines provided in the owner's manual for your computer? If your response to that question is "What manual?" then you're not alone. Many computer systems come with little or no documentation. Any manuals you did receive were probably put straight into storage in a big box with your other hermetically sealed books. If you peel off the shrink-wrap and read through one of these books, you will usually find only the most minimal guidelines for keeping your computer running smoothly and reliably.

Just like your car, your computer systems require regularly scheduled monitoring and maintenance. Unlike your car though, a computer comes out of the box in need of help. Even a new name-brand computer requires numerous security patches and fixes. This goes for more than just the PC on your desktop. Your servers, laptops, networking gear, peripherals, etc. — they all need a constant level of upkeep to perform at their best.

You'll find a sample plan for monitoring and maintaining your systems at the end of this article. Before implementing such a plan, there are some important points to understand.

First, there is no one-size-fits-all maintenance plan. There are many different types of monitoring and maintenance activities to consider, and the proper schedule for doing them will always be a matter of debate. As with most technology decisions, the level and scope of maintenance you perform is a matter of policy. Only you and your information technology consultant can weigh the costs and benefits, and determine the type of plan that best suits your organization.

Second, while following a sound monitoring and maintenance program isn't a panacea,

it will prevent many smaller problems from turning into bigger ones, and will eliminate some problems completely. However, a maintenance activity itself may sometimes cause a problem. This certainly shouldn't deter you from installing the latest Microsoft security patch, but to minimize potential problems you should test it out on one or two computers before you install it on your boss' laptop.

Finally, don't get discouraged. Nobody said this was going to be easy. Getting up to speed may take a considerable amount of work — especially if you haven't followed a regular maintenance program before. On the bright side, it does get easier and consumes less time once you're on top of things. Plus, there are numerous tools and methods for automating many of the activities. There's also no shortage of professional information technology consultants willing to do the work for you or to teach you how to do it yourself.

A word of caution: None of these activities should be attempted unless you know what you are doing and have good system data backups.

The Schedule

The monitoring and maintenance schedule is divided into daily, weekly, monthly, quarterly, semi-annual and annual activities. It's best to lay out the schedule in some type of calendaring system so that you know what needs to be done every day of the year. Some of the activities may be more time consuming than others or may require some scheduled downtime. Put reminders into your calendar at least a week beforehand so you can give yourself (and your organization) some time to prepare and plan. Keep a checklist and notebook so you can manage and track your work.

• **DAILY**
Backup status and

rotation – Check your daily backup and note the date and status (success or failure). Write down the overall size of the backup and total run-time and compare it against prior results. A sudden increase or decrease may indicate a problem. Insert the proper media indicated for that day's backup.

Clean tape drive – Check your tape drive and run your cleaning tape if indicated.

System logs – Review your server and workstation operating system logs for abnormal errors and warnings that might indicate specific problems.

Server disk space – Write down the used and free disk space on all server hard drives and compare it to past days. A large increase or decrease may indicate a problem.


Anti-virus updates – Anti-virus signature/definition files should be checked for on a daily basis and any updates should be installed on all servers and workstations.

• WEEKLY

Verify anti-virus updates – Verify that your

(continued on page 29 ►)

**Tip
the
scales
in
your
favor.**


**Legal
Placement
Services**
A division of
Personnel Specialists Ltd.
740 N. Plankinton Ave.
Suite 430
Milwaukee, WI 53203
(414) 276-6689
FAX (414) 276-1418
www.legalplacementservices.com

Serving Milwaukee's legal community with integrity since 1979.

process for downloading and updating antivirus software updates is working as expected and that everything is functioning normal.

Full anti-virus scans – Complete a full anti-virus scan on all servers, workstations and groupware/e-mail systems. This will help to detect a virus that may have slipped through the cracks or a new virus that wasn't detected by the signature/definition files available at the time of infection.

Review Other Logs – Check system logs and events on firewalls, managed network switches, and print servers for abnormal errors or warnings that may indicate a problem.

Software security updates – Review and apply any critical security updates for your server and workstation operating systems. Whether you run Microsoft Windows, Novell Netware, Mac OS X, or some form of Linux/Unix, security holes should be patched.

• **MONTHLY**

UPS test – Make sure your uninterruptible power supply is functioning properly and calibrated to your power needs. Depending on the load, many UPS batteries should be replaced every 3 years. Reboot your entire network – All devices including servers, workstations, routers, hubs, switches, network print servers, etc. should be properly shut down completely and then restarted. Clear out temporary files – Review and clear temporary holding spaces such as temporary files, bad mail folders, anti-virus quarantines, etc.

• **QUARTERLY**

Check disk and defragment – On servers and workstations, run standard disk diagnostics and file system integrity checks to repair any physical or logical errors.

Defragment your drives to improve performance and reliability.

Update emergency recovery disks – Many server operating systems allow you to create special boot floppies or drive partitions to help recover from certain types of failures. Systems may change over time, so make sure your recovery system is up-to-date.

Test restore of tape data – Restore a few files from a recent backup to ensure you are getting the data backups you expect.

Update workstation software – Review and apply any major service packs or maintenance releases for your standard software packages (i.e. your office suite or accounting system), and for hardware drivers (i.e. your video card or printer).

• **SEMI-ANNUALLY**

Tape replacement – Backup media eventually wears out. Review and replace as necessary.

Surge protection – Make sure all devices are plugged into working surge protectors. Also, because surge protectors can degrade over time, review and replace them as necessary.

Hardware tune-up – Open the cases on servers and workstations, blow out all dirt and dust, and check to see that all cooling fans are operational and spinning freely. Also, make sure the internal cables are snug and all add-in cards and memory are properly seated.

Update server software – Review and apply any major service packs or maintenance releases for server operating systems and software for backup, anti-virus, and groupware/e-mail servers, etc. Don't forget to include drivers for hardware such as video cards, network cards, disk devices, etc.

BIOS/Firmware updates – BIOS and firmware is another name for the software embedded in certain chips on computer motherboards, RAID cards, routers, firewalls, print servers, etc. Like any software, it may get updated with new features, bug fixes, and security patches. Review your versions against current ones and update if necessary.

Data purge – Review overall disk usage and purge or archive old, redundant or otherwise unnecessary data.

Data reorganization – Review how data is being stored and reorganize your information to ensure conformity to your organization's standards.


Database maintenance – Run maintenance/patch and re-index utilities for all systems that use an underlying database for primary storage such as your e-mail, accounting, or customer information systems.

General organization – Take some time to make sure you have all your system documentation, media, proofs of licensing, etc. in order and current. User Administration – Check to see that you've deleted or de-activated any users no longer with your organization. Make sure to save any of their old data if you still need it.

• **ANNUALLY**

Verify all licensing is in order – Make sure you have enough purchased and activated licenses for your organization.

Budgeting – Plan for the purchase and replacement of any defective or aging equipment.

Systems review – Meet internally and with your information technology consultant to review any changes in your business that might affect your computer systems. 



800.222.0510
www.aslegal.com

ALL-STATE LEGAL

ALL-STATE LEGAL specializes in converting your challenges into opportunities with more than five decades with an exclusive focus on the legal profession nationwide.

Stationery ■ Filing ■ Legal Specialties
Over 30,000 Law Office Essentials