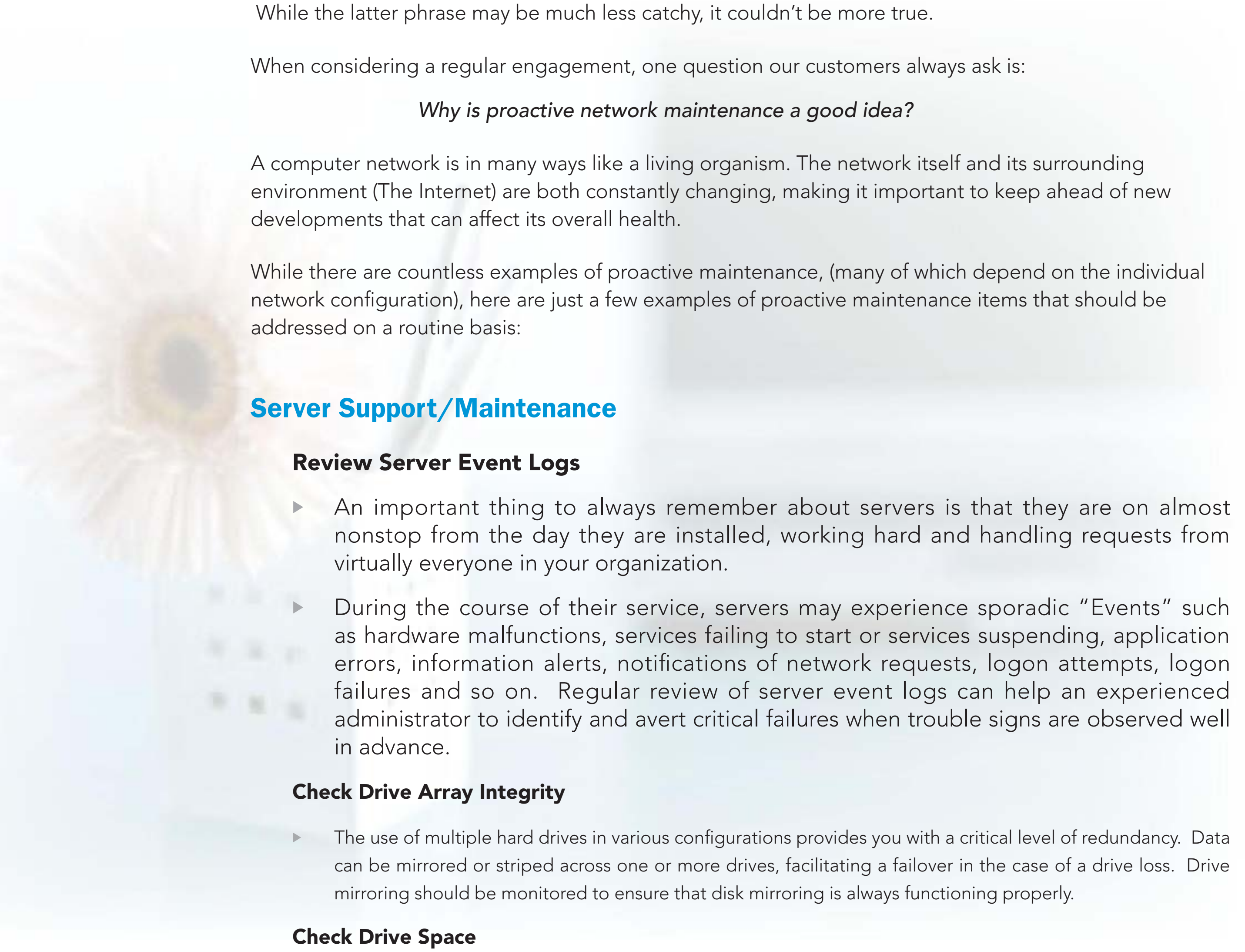
Question: SHOULD I CONSIDER *PROACTIVE* Network Maintenance?

It's been said that an ounce of prevention is worth a pound of cure. In technology, one might say that a few minutes of cleanup and updates are worth hours of recovery time and lost productivity.

While the latter phrase may be much less catchy, it couldn't be more true.

When considering a regular engagement, one question our customers always ask is:

Why is proactive network maintenance a good idea?



A computer network is in many ways like a living organism. The network itself and its surrounding environment (The Internet) are both constantly changing, making it important to keep ahead of new developments that can affect its overall health.

While there are countless examples of proactive maintenance, (many of which depend on the individual network configuration), here are just a few examples of proactive maintenance items that should be addressed on a routine basis:

Server Support/Maintenance

Review Server Event Logs

- An important thing to always remember about servers is that they are on almost nonstop from the day they are installed, working hard and handling requests from virtually everyone in your organization.
- During the course of their service, servers may experience sporadic "Events" such as hardware malfunctions, services failing to start or services suspending, application errors, information alerts, notifications of network requests, logon attempts, logon failures and so on. Regular review of server event logs can help an experienced administrator to identify and avert critical failures when trouble signs are observed well in advance.

Check Drive Array Integrity

- The use of multiple hard drives in various configurations provides you with a critical level of redundancy. Data can be mirrored or striped across one or more drives, facilitating a failover in the case of a drive loss. Drive mirroring should be monitored to ensure that disk mirroring is always functioning properly.

Check Drive Space

- Running out of hard drive space can bring business to a halt. Large, unauthorized downloads can consume space quickly if not kept in check. When a server becomes full it may become unusable, even crash. If a "full" server is used for email storage, new emails may be returned to sender as undeliverable. These are just a few of the reasons why checking drive space availability on a regular basis is very important.

Delete Temporary Files (Server And Workstations)

- Computers create what are known as temporary files when browsing the Internet or accessing various files. While these files are important at the time the primary file is in use, they serve little purpose afterward, and consume valuable disk space. Deleting temporary files on a regular basis helps machines to work much more efficiently.

Check Backup Status

- Upon completion of your regular backup process, your backup software will typically display one of several messages pertaining to the success of the backup job. Such messages include "Complete", "Incomplete" and "Failed". (In some serious cases, backup jobs may also suspend and give no message.)

- All of our customers are advised to have someone within their organization check the backup status on a daily basis. With that said, in nearly eight years of being in business, we've observed that over half of the failed backup jobs reported are discovered by our staff during routine spot checks, many after having failed for days, even weeks in a row. In addition to causing considerable frustration, lost data can cost hundreds of man hours to recreate. For this and other reasons, it's always a good idea to have a second set of eyes spot checking your backup

Review Backup Log Files

- Whenever a system backup is performed, your backup software produces a detailed log of events occurring during the backup process. These logs include lists of open files encountered, corruption, file security restrictions, etc. Such problems can prevent specific files from being archived, even when an overall backup may be classified as successful. Periodic reviews of backup log files are the only means of identifying these errors and determining whether or not they warrant further investigation.

Perform Test Restore Of Backup

- Unfortunately, backup logs and reports aren't always 100% accurate. For this reason, we recommend that periodic test restores be performed to verify the integrity of archived data.

Check Virus Definition Update Status (Live Update)

- Most of our customer systems are configured to leverage Symantec's Norton Antivirus Corporate Edition. This highly effective antivirus suite is configured to automatically check the Symantec site for updates containing definitions for new viruses that could potentially affect your system. New virus definitions are downloaded by the server, and subsequently pushed out to user workstations. Since viruses are capable of creating so much damage, it is important that the Live Update functionality of Norton Antivirus be checked regularly to ensure that the system is updating properly, and to ensure that it is pushing virus definitions out to all user workstations.

Update Antivirus Software

- Not unlike other software products, antivirus software is subject to code flaws, security exploits, software conflicts and other gremlins of the technology world. Symantec often releases patches and other updates to its Norton Antivirus product. Your Norton Antivirus software should be checked regularly, and outstanding patches should be reviewed and applied as needed.

Software Updates (Server & Workstations)

- Software developers constantly release updates or "patches" to their products. These patches are designed to do a number of things, such as correcting bugs or errors in the original product, correcting compatibility issues and plugging newly discovered security exploits that could be used to compromise the system. Microsoft frequently releases patches to its operating systems, and sometimes rolls them into larger updates known as "Service Packs". Unfortunately, some fixes actually cause new problems while fixing others. For this reason, it's important to have a skilled professional keeping tabs on what fixes are available, and applying them as needed. Patches are released for everything from office and financial software to virus protection software, printer drivers, and even video games. If it's been written, there's probably a patch for it. Knowing what patches are available and applying them when they're needed is a critical for overall network health and security.

Workstation Maintenance

Spyware Removal (Workstations And Servers)

- Over the past year, spyware has gone from being a nuisance to a crippling and pervasive disease. Web sites everywhere practice planting tiny bits of code that collect data about user Web surfing history and habits. These unwelcome and unauthorized routines, known as spyware, report back to their originators, who use the information in various ways. We've found that an average PC that's been in service for a month or more will often have upwards of a dozen or more pieces of spyware installed. Since spyware is constantly collecting information and reporting back to it's creator, it not only compromises user privacy, it consumes CPU time and Internet bandwidth, making your PC run slower and decreasing your Internet access speed. Some spyware can cause increased pop-up ads, making Web surfing near impossible. Machines with dozens of harmful spyware entries often fail completely, requiring a major overhaul. For this reason, routine spyware scanning and removal is a critical part of maintaining any workstation with an Internet connection.

Spyware Mitigation (Workstations And Servers)

- In addition to running various utilities designed to identify and remove spyware, there are programs that help prevent spyware from being installed in the first place. Unfortunately, since new spyware applications are constantly being created, the programs to help prevent spyware infestation must be constantly updated. Nonetheless, proactive blocking of spyware can go a long way towards ensuring the overall health of a system.

Delete Temporary Files

- Computers create what are known as temporary files when browsing the Internet or accessing various files. While these files are important at the time the primary file is in use, they serve little purpose afterward, and consume valuable disk space. Deleting temporary files on regular basis helps machines to work much more efficiently.

Software Updates

- Software developers constantly release updates or "patches" to their products. These patches are designed to do a number of things, such as correcting bugs or errors in the original product, correcting compatibility issues and plugging newly discovered security exploits that could be used to compromise the system. Microsoft frequently releases patches to its operating systems, and sometimes rolls them into larger updates known as "Service Packs". Unfortunately, some fixes actually cause new problems while fixing others. For this reason, it's important to have a skilled professional keeping tabs on what fixes are available, and applying them as needed.Patches are released for everything from office and financial software to virus protection software, printer drivers, and even video games. If it's been written, there's probably a patch for it. Knowing what patches are available and applying them when they're needed is a critical for overall network health and security

Network Hardware Maintenance

Hardware Updates

- Not unlike your computers, updates are often released for hardware components as well. SonicWALL firewall devices have built in operating systems and firmware, which is updated from time to time. This also stands true for Internet routers and even some network switching equipment. Keeping current on firmware updates can help your network remain efficient and avert disasters down the road.

Physical Hardware Checks

- Ever noticed all those lights on various devices in your company's server room? A light next to the wrench icon on your SonicWALL could mean trouble brewing. Router and modem lights can tell you whether you have a serious problem, or if your provider is just down. A rapidly flashing link light on a switch port can indicate a busy user, or it can also mean a virus infection or failing network card. It takes an experienced engineer to know the difference. Keeping a constant eye on your hardware can mean the difference between proactively replacing it and waiting several days for the part to arrive once your system has failed.