

In This Issue

[Disaster Recovery](#)
[Web traffic - Should I be monitoring?](#)

Quick Links

[Parallax Solutions Online](#)

About Us

Parallax Solutions is a health information technology consulting firm located in the Waterloo/Cedar Falls area. What we are trying to bring to the table is a clear understanding of how medical offices can utilize hardware and software to effectively manage their electronic information.

Join Our List

[Join Our Mailing List!](#)



I hope you have enjoyed this issue of our newsletter. If you are concerned that your network isn't living up to its potential, give us a call.

Sincerely,

Steve Bantz
Health
Information Technology
Consultant
Parallax Solutions
319.235.8034

Featured Products

[SonicWall](#)
[Symantec Backup Exec](#)

Issue: # 3

July 2008

Welcome to the latest edition of our technology newsletter. I'd like to take a moment to introduce you to our newly re-designed website, located [here](#). We have freshened the look and added a bit more information about the company. If you know of anyone interested in trying our services, feel free to pass the link on to them.

Steve Bantz

Disaster Recovery - Do you really have a plan?

With the recent flooding in my own hometown, it got me wondering how many businesses were prepared for a natural disaster. If the business and all related electronics were under water, what would happen to the information? Many companies don't even realize they had been lacking a disaster recovery plan until it is too late.

At the very least, you should always ensure that you have offsite backup of your critical data. This is as simple as taking the last good backup home with you each evening. In the event of a natural disaster, having a backup tape stored offsite may be your only savior. However, having a single tape offsite is not always failsafe. In the event of a large scale natural disaster, if the tape is stored offsite within a small geographical radius of the company server, chances are it could meet the same fate as the company server. For this reason, many companies choose electronic offsite storage. Using this method, data can be sent over an encrypted Internet connection to a repository located in another state. Obviously, this lessens the chance of losing both the server AND the backups to the same natural disaster. This should not be a substitute for regular local tape backup. Think of it as an extra measure of protection and an excellent contingency plan.

If you lose your server equipment to a disaster, you could conceivably be back in business in short order if the data is available on a tape. Some backup software has built in one button disaster recovery, allowing you to boot to a tape and restore the operating system and data in one step. As a contingency, you should have all of your servers well documented so that you can recreate them from scratch and restore the data itself. Servers need to be well documented because they are rarely ready to go right after a fresh installation of a server operating system. There is usually plenty of customization needed for it to become 100% functional again.

One more tip. If you do lose computer equipment to flood waters, don't just throw them away. The information on the hard drive could still be readable and you don't want that

falling into the wrong hands. If the PC isn't salvageable, make sure you remove and thoroughly destroy the hard drive. This [link](#) contains tips on destroying your hard drive. Of course, use at your own risk since these actions cannot be reversed.

In the next issue, we'll dig a little deeper into what you need to do to protect your invaluable information.

Should you monitor web traffic?

A good percentage of spyware and malware comes from browsing websites that are not deemed business related. If you don't have a good malware prevention and remediation solution on your network, this ends up being a huge security loophole that you cannot afford to leave open.

Many firewalls, such as the SonicWall series, have a subscription service that allows you to block access to websites on the Internet that are not business related. Of course, you can customize it to suit your needs so that you are not blocking sites needed by your staff.

Do you need to restrict access to everything? Not at all. Studies have shown that workers are more productive after a ten minute "surfing" break than they are in an equally timed coffee break. Solutions from Websense, SonicWall and other vendors are tuned to allow users to get to a vast majority of sites they want, while blocking content from sites with malicious intent. You can fine tune as needed to provide your users with a web experience that allows a certain degree of freedom while still protecting your workstations and servers from malware.

Keep one thing in mind when allowing the freedom to browse the Internet. Patients/customers passing by a workstation might catch a glimpse of something that might not be appropriate in a workplace setting. Luckily, most web filters come pre-set with blocks on offensive and vulgar material while still allowing "monitored freedom."

✉ **SafeUnsubscribe®**

This email was sent to administrator@dvineinc.com, by solutions@parallaxolutions.net
[Update Profile/Email Address](#) | Instant removal with [SafeUnsubscribe™](#) | [Privacy Policy](#).

Email Marketing by

