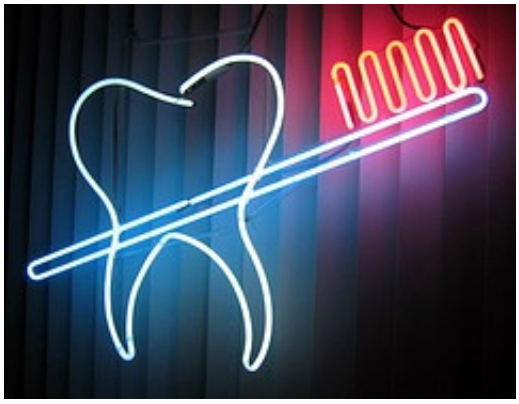
3 Backup Basics Every MSP Should Deliver

FEBRUARY 06, 2014 ROBYN WEISMAN NO COMMENTS



My friend, a dentist who we'll call "Dr. B," is in a bind. He has a nice practice in a large city, and he isn't afraid of technology. For the most part, his business runs on an in-house server, though he does keep paper-based patient charts as a backup. This server holds apps and data for:

- Patient records
- Dental-specific practice management software (here's an example)
- X-rays and radiographs

Dr. B backs up his in-house server nightly and takes that backup volume home with him. He also has a backup at the office in case anything goes down. Although he has yet to experience a hard drive failure or some other glitch that could hurt his business, he knows his backup and disaster recovery strategy is less than ideal. He admits he doesn't have a way to ensure that his backups don't fail when they're needed. Meanwhile, HIPAA's recently enacted Omnibus rule requires his practice to encrypt patient-related data and provide his patients with electronic records on demand, among other conditions.

Dr. B worries his small business doesn't have the resources to take charge of all these issues related to storage, backup, and recovery, and so I'd love to recommend a great MSP that's geared toward his profession. But before you try to get in touch with me, here are three key requirements I would expect to see addressed.

1. Quick, Secure Initial Backup

As I discussed in my previous post, I think you should have multiple backups stored in multiple locations, including onsite and in the cloud. The former is easy, especially when you use a product like StorageCraft's ShadowProtect. The latter is more problematic, at least at the get-go. In a blog post written last year, StorageCraft alliance partner Highly Reliable Systems points out that backing up a volume locally can be as much as 1,000 times faster than doing so over the Internet:

> *How long do you guess it would take to upload 100 Gigabytes of data if you had a fairly typical DSL with 3Mbps download/512Kbps upload speed? [T]he FASTEST you could ever experience would be 19.5 days! … The same 100 Gigabytes transferred to Direct Attached Storage (DAS) using USB3 or eSATA and a large hard drive or RAIDPac would take about 15… to 30 minutes.*

An MSP that wants Dr. B as a customer must be able to offer him a secure, "seed" hard drive volume that he can use to back up his data and send securely to the MSP's servers or to StorageCraft Cloud Services.

2. Painless, Automated Incremental Backup

Under his current backup and recovery strategy, Dr. B is not protected should his system go out at, say, 4:30 PM on a workday. Because he only backs up nightly, a hard drive failure means that he's lost all the data inputted for that workday—all the patient charts, insurance forms, X-rays, and everything else. He needs a way to perform incremental backups that will only add new files and changes to his backup disk image without impacting his overall backup or the performance of his system during business hours. StorageCraft's ImageManager solution comes with several tools to help out with these issues. The intelligentFTP (iFTP) tool knows to back up only new parts and alterations to his backup disk image without altering the integrity of that image. Moreover, iFTP may be configured so that it complies with file retention policies, something especially useful for dentists in this age of increased regulations.

ImageManager also offers bandwidth throttling so that maximum transfer speeds can be regulated depending on the time of day. During peak business hours, data will be transferred at a slower rate than during the middle of the night. And the ability to do this automatically means that Dr. B doesn't have to manually perform nightly backups of his data.

3. Verified Backup Images

Of course, the aforementioned requirements are meaningless if Dr. B finds himself with a passel of

unverified backups. The MSP responsible for backing up Dr. B's disk images and files needs to provide continuous verification, so problems like data corruption or other errors prevent those backups from providing failover and disaster recovery protection. Fortunately, ImageManager provides continuous verification functionality to ensure disk images are recoverable, as well as its HeadStart Restore feature, which can pre-stage a backup image as a VM that lets you restore your system within minutes.

Small businesses like Dr. B's practice want great backup, disaster recovery, and failover solutions so that they can focus on what they do best, but they often don't know where to turn. If you can address these issues in a way that makes sense to Dr. B, you will find yourself with a great customer. And if you can offer a bit more handholding, I will introduce you to my dentist, who, with the exception of dental X-rays, has yet to digitize *anything.*

Photo Credit: get directly down via Compfight cc

Robyn Weisman

Robyn Weisman has written about technology for over 15 years, specializing on IT-related topics, such as data recovery, cloud computing, and hybrid IT environments. Her email address is robyn[at]robynweisman.com."

More Posts

Follow Me:

Posted in: Business Planning, Disaster Recovery Tags: backup, curation, disaster recovery, IT industry, MSP