Business continuity and IT management (part 2)

By Lorne Lavine, DMD

In part 1, we looked at ways to monitor the network 24/7 and be alerted to problems.

Well, what if there’s a true disaster — fire, flood, theft — and your entire network is destroyed?

I’ve just developed a complete paradigm shift in how I approach data backup and protection. Let’s look at a typical scenario. An office has a dedicated server and perhaps eight to 10 computers throughout.

The office backs up nightly to an external hard drive or tape and that device is removed from the office every evening and taken offsite.

So, if anything ever happens to the office server, you’re protected, right? As I’ve found out over the past few years, the answer is usually no.

The problem isn’t that your data is offsite and protected — you’ve got that covered. The problem is how long it takes to recover from a disaster.

If someone accidentally deletes a file or your practice management data becomes corrupted, that’s easy — just restore the missing or corrupted file from your backup. You’re still able to run the practice with no downtime.

But, what if something happens to your server or main computer to make it non-operational? Motherboards can get destroyed by power surges. Servers can be stolen or ruined by fire or flood.

If you don’t have a server that is running, what do you do with the backup? That’s the real problem that had me worried for a long time — how long would it take for a support technician to get an office back up and running if the server was gone?

Unfortunately, I found out the hard way with a few of our clients that the answer is: too long.

The fastest we were able to get an office up and running was 24 hours, and that was because they were able to go out and purchase a brand new server locally.

The other offices averaged 48–72 hours, and a few were longer than that.

That’s the real problem that has been overlooked by many dental offices when it comes to their backup system: not if the data is protected, but how much downtime will the practice suffer if something goes wrong?

Consider that if your server is down, you are down. You cannot schedule patients, cannot take digital X-rays, cannot create treatment plans, cannot access patient data — you’re literally dead in the water.

But what if there was a system available that could guard against this? What if there was a way to be back up and running within 50–60 minutes, even if your server was destroyed?

What if you could combine this system with automatic backup to an offsite location that required no input from you or your staff? Wouldn’t a system like this be valuable for any dental practice?

Systems like this have been available for a few years for large corporations as they really couldn’t recover from a disaster without it.

The concept is called “business continuity” and that seems to be a proper description: being able to continue to run your business even in the face of a disaster to your technology systems.

The main deterrent for a dental practice to incorporate something like this was cost, but the costs have now dropped enough to make it a practical option.

Business continuity and IT management (part 2) is a valuable resource for any dental practice looking to protect their data and ensure minimal downtime in the event of a disaster.

About the author

Dr. Lorne Lavine, founder and president of Dental Technology Consultants (DTC), has more than 20 years invested in the dental and dental technology fields. A graduate of USC, he earned his DMD from Boston University and completed his residency at the Eastman Dental Center in Rochester, N.Y. He received his specialty training at the University of Washington and went into private practice in Vermont until moving to California in 2002 to establish DTC, a company that focuses on the specialized technological needs of the dental community.