IS YOUR ORGANIZATION AT RISK WITHOUT A SUFFICIENT BACKUP AND RECOVERY SYSTEM?

What if you lost physical access to your office? Could you be back in business at another location within a couple of days? If not, you should explore cost-effective, reliable backup choices.

No one ever thinks it could happen to them. Yet, we have all seen and possibly experienced the devastation that can be caused from natural disasters, accidental file destruction or even terrorist attacks. Everyone needs to think about what would happen if all business operations suddenly came to a halt. Could your business recover if you lost all of your data?

Data backups is a subject so overdone that it has become “incidental”. Today, everyone knows that they need to be taking backups of their system data and the big issue today is that everyone “assumes” that this is being done at their companies. Network people are hired to install the network and “everybody” naturally assumes that this was part of the set-up and that somehow this is magically being taken care of. This is a big mistake.

All companies, large and small, need to have a secure backup and recovery plan in place. The key word here is perhaps “recovery”. Having been in the software business for over 20 years, I am no longer amazed when companies routinely perform backups and yet never test them to see if they are actually working. When it comes time to restore, it’s an unpleasant surprise to find out that the backup wasn’t really backing anything up or it was not backing up the correct files.

Having a sound plan in place extends farther than simply running a tape every night (which by the way is mandatory step one in the process). In addition, tapes need to be rotated each night so that the same tape is not being used over and over again. One never knows when one may need to recover data from a couple of days ago because the current data is not good. A tape should exist for each day of the week that the system gets backed up (minimum 5 days). Besides the rotation, copies should be kept off site, preferably in a safety deposit box and/or another secure location that is not in the immediate area of the office. It should be a site that can be accessed quickly if data needs to be retrieved. Ideally, the off-site copy should be refreshed at least once a month.

Besides the daily backup tapes, backups should be taken at the end of the month, quarter and year. These backups should never be used again and should be clearly labeled in the event that you need to access the data. If you are doing payroll, the government can call at anytime, even in several years. You want to be prepared. Not being able to produce the data can mean penalties, legal and accounting fees.

Running a backup tape and keeping it off site is just the beginning of the process. Backups need to be periodically tested to ensure that data is being copied. A knowledgeable, technical person should be in charge of this task. The line, “you can never have enough backups” is very true. However, testing that the backup you are taking is “good” is equally important.

Having a good routine for taking, testing and storing backups is critical. If your data is protected, even if you do not have access to your office and even if your server is destroyed, you can always restore on another system at another site. We had customers that had offices near ground zero and were unable to return to their buildings for quite some time. In a couple of days, with good backup tapes, they were able to restore to new hardware at another location and were back in business within a couple of days. Being prepared is the difference between business recovery and business failure.

In addition to the physical backup plan, every company should have a plan in writing that outlines the steps that the company will take to recover and resume work at locations other than the office. The plan should encompass not only the steps that will be taken to restore the data, but how and where the employees will access the data. If remote access is possible how would that option work? Would multiple offices be blended into one temporary central location? Several possibilities and solutions should be available so that most situations can be addressed without a last minute appeal for a solution.

A disaster represents many challenges, most of which cannot be prepared for. Restoration of data and resumption of use of the data is one thing that can be arranged. Unfortunately, this type of plan is traditionally not a top priority and considered secondary to the core business operations. The primary point to keep in mind, however, is that it is essential to securing and preserving core business operations. The smart business choice is a solid backup and recovery plan.