The

Broadcasters' Desktop Resource

www.theBDR.net ... edited by Barry Mishkind – the Eclectic Engineer

Doing IT Right

Ensuring Your Data is Safe

[September 2015] Some recent reports of radio stations being attacked make this a good time to update your policies on backups and computer security.

Consider for a moment what would happen if your automation system died tomorrow – or if your bookkeeper suddenly was locked out of the computer - with a demand for money. Would this crimp your style in any way?

If so, **this** is the right time to check and ensure you have a good backup protocol. Just as critical: have you spot-checked lately to ensure your backup works? Why? Having a backup does no good if you cannot use it when things happen.

BACK IT UP!

"Backup! Backup! Backup!" Every good IT person preaches it – and has a good plan to make certain that all important data is backed up.

… and every station employee has an excuse as to why it cannot done right now.

Nevertheless, the need for backups really cannot be over-emphasized. It could be as simple as saving your address book, as complex as the field data acquired during a directional antenna proof, or as critical as the legal details relating to a contract for operating or selling a business.

EASIER THAN IN YEARS PAST

In the early days of computing, when 5 MB hard drives were large and expensive, tapes were still the primary means used for backing up – using a manual and lengthy process.

One oft-told story dealt with a fired employee who erased the company's financial data tapes before leaving. The business was said to have gone bust quickly, as all the accounts receivable were gone and the company was reduced to asking clients if they owed money; few responded in a positive manner.

Today, with more and more data stored on hard drives and flash drives than was ever conceived – including programming and technical files as well as graphics and financial information – a hard drive crash or flash drive corruption can destroy many times more critical data.

Bottom line: losing the contents of a hard drive could represent many hours of work and possibly even the loss of irreplaceable data.

BACK IT UP NOW!

Since your operations could be crippled if you do not have good backups, the key to preventing data loss is making sure important information is safely and securely backed up.

Is your data safely and securely backed up? We will wait a moment while you go and check.

Seriously, though, there are many options for backing up data, including secondary hard drives, network storage, external hard drives, off-site drives, flash drives, laptops, CD ROMs, and DVD copies. If you have an Apple machine, the "Time Machine" might work well for you. It just sits there and does incremental updates to all your files, so you can even go back and easily retrieve a version from earlier in the day, week, or month.

Of course, each option has its particular benefits and liabilities. Let us take a look at these options and how they can benefit your situation.

DOING IT RIGHT THERE

In-house storage is the easiest to do, especially if it is automated, but it is also subject to virtually the same dangers as the original: theft, hackers, power surges, fire, flood, etc.

Some companies rotate media. Others burn a CD or DVD each week. Still others utilize a laptop as a dual media item: they can save the data and can carry it along wherever it is needed, even if the studio must be abandoned in an emergency.

Another solution is to arrange “ghost” drives, so that in case of hard drive loss or massive infection, the operating system and key files can be quickly reloaded on a new hard drive or machine, with data files loaded from the server.

There are many software packages and home-built scripts in Windows, Linux, and others that will automate backups. Choose one that works for you, or ask a friend for a recommendation. Some servers have built-in apps, including RAID systems, to do the job.

A CAUTION ABOUT LOCATION

But, depending upon your location, just putting the backups in what looks to be a safe place (or on the second floor, for example) may not be enough.

Sometimes it is a hurricane, a fire, a flood, or a tornado that wipes out a community. That might simply destroy your backups entirely. Or, if they are on a server, loss of power could prevent access for a lengthy time.

And there is one more reason for not keeping the backups close and on the LAN or WAN: malware. Just one current piece of malware (of many) running around, the so-called ransomware like *CryptoWall* or *SynoLocker*, could easily contaminate any computer or NAS (Network Attached Storage) it can find with a shared drive letter, corrupting or destroying backups.

For that reason, having separate networks on site that can be completely isolated could reduce the danger of destroyed (or hacked) data and, reduce the time to restoration of the data.

LOCATION, LOCATION, LOCATION

As you give thought toward protecting your valuable data, that old line should come to mind: “Location, Location, Location.”

One option is to use special software or scripts to copy key files to an isolated backup drive. Depending upon your system, It is not always necessary to backup applications, just the data files, word documents, or spreadsheets. Should you backup the music files? That would depend upon your system; get advice from your automation system provider.

For example, some LANs already extend to transmitter sites for on-site Internet access or remote control. WANs may lead to a server in another location, perhaps another state.

These can be good ways to do off-site backups for key data – even an entire day’s automation can be mirrored this way, so that in case of trouble at the studio, operations can continue with almost no interruption.

It does require a bit more effort to deliver data this way to other locations – even if it is “only” transferred via IP – *and to make sure* it was transmitted correctly and intact, and is secure at the storage point. This is not an area to downsize staff.

For maximum security, just like a standby transmitter not normally connected to anything, planning and building a “mirror” computer and external site storage for applications and data files that can be completely disconnected from the world makes it much less likely for either to be lost at the same time as the original.

ANOTHER POSSIBILE OPTION

Although high speed Internet connections make it possible to easily accomplish backup and off-site transfer, some Internet sites offer another solution.

Internet email sites have long offered storage of email and, with a little effort, data files. Additionally, there is now a wide range of locations, from photo-sharing sites to sites devoted to data storage have made it easy to upload anything from your vacation pictures to business files. *Dropbox* is one of these sites, used by many to store or share files.

The big question, though, is how safe are your data files?

SECURE … AND ACCESSIBLE?

While you may have quite a pile of files saved somewhere on the Internet – it is now called being "in the "Cloud" – a disturbing trend has shaken the confidence of some.

One might call it a "shaking out" of on-line storage providers as some close down or sell out.

Many sites offer some free storage, some with many Gigabytes and features available for a fee. But between hardware, infrastructure, support personnel, and bandwidth, it can cost as much as $100 to maintain a terabyte of data. (A common problem: a good idea does not necessarily make a good business plan.)

As these sites burn through their cash, some find there is not enough upside to keep them going. Several have shut down with little or no warning to users. Other companies, which make money selling copies of photos, for example, seem to be somewhat better off.

Some big names have tried but are no longer offering services – among them, AOL, Kodak, Hewlett-Packard, Sony, and Yahoo – as well as a number of smaller firms. According to reports, some users have lost hundreds, even thousands of pictures when the storage site they were using was shut down with as little as 24 hours' notice.

Even if you learn of the impending shutdown, the rush of other users trying to retrieve their files can slow or even crash the servers, making it hard to recover valuable files. And then there are the other potential potholes: server outages, sometimes short, sometimes lasting for hours, that could prevent you from accessing anything stored in the Cloud.

As a result, relying solely on such Cloud sites could present you with a real data pain if you need something quickly and cannot get to it. Think personnel files, for example.

WHAT? ME WORRY?

So, is your data safe? Is it at risk? Has it already been lost?

There is no central list of sites that are in trouble. Fortunately, the larger companies, like AOL, normally give users several months' warning before closing sites like AOL Pictures.

Another tactic that is being used by those that remain is to start charging for storage. For example, one site has instituted charges of $5 to $20 per year, depending upon the size of the data stored. Furthermore, most sites post warnings about potential data loss, especially for those who do not sign up for a pay-for-storage account.

****** CAUTION ******
ROUGH AND BUMPY ROAD AHEAD
DIGITAL ALERT SYSTEMS CAN HELP
Digital Alert Systems
Your Partner on the Road to EAS & CAP compliance
585-765-1155
Digital Alert Systems
Digital Alert Systems DASDEC™-II

Therefore, if it has been a while since you last checked your upload site, it might be a good idea to check on it from time to time to see if there are any policy changes.

At the same time, spot check your data to ensure its integrity. As we mentioned before, retrieving a corrupted file does not help much in an emergency.

PROTECT YOURSELF AND YOUR FILES

Whether or not you use a Cloud site, a very good recommendation is to keep another set of copies of important things in a safe place.

After all, what are you going to do if a company 3000 miles away (or on another continent) has a hard drive crash and/or disappears, along with your files? Even if they could be found, can money replace what you stored?

While it is likely they themselves make backups of all their users' files, ultimately you are still the one responsible if files are lost. And regardless of their practices, how do you *know* the files are not corrupted? It has happened.

In other words, it is essential that you regularly stop and test your backups, wherever they are, perhaps doing a partial restore, to ensure the integrity of your data is more than just "hope" that is will be there when you need it.

Or, to consider another "worst case scenario:" what about the safety and security of your personal files if your employer suddenly decides to downsize tomorrow and you do not get ti return to access your desk machine?

BEST PRACTICES

The best advice, then, is to consider on-line storage as a convenience.

Use it. But remember: "backup, backup, backup." And "Location, Location, Location." Even so, be sure to periodically make a safety copy and store it somewhere else.

Before concluding, let us emphasize that backup protocols require setting aside enough time and the right personnel to do the job correctly. Yes, everyone is busy; with reduced staffing, few are sitting around with nothing to do.

As one person put it: *"Think of it this way: What is your commercial inventory worth and how long could you manage without it? Put in that perspective, a fully configurable firewall and a few hours of IT expertise are well worth it. It's as if you purchased an insurance policy."*

Simply telling someone to make backups is not enough. They need to understand more than IT, they need to understand the structure of how a broadcast facility works, and approach the task with that in mind. That often requires time and attention from the engineer. So help him get this job done. There are many critical "do it now" jobs on his plate, but this is not one to let slide.

Bottom line: a good mixture of local backups, along with on-line storage, a CD, DVD, or external hard drive with your business records or your family's pictures and history placed in a safety deposit box will go a long way toward preventing any catastrophic loss. -- **BDR**

- - -

The BDR offers many articles and tips to help you deal with the problems of keeping everything running. If you have not done so, please take 30 seconds to sign up here for the one-time-a-week BDR Newsletter and we will keep you up-to-date.

Return to The BDR Menu