Tips & Tricks #39 – Backups are Critical

We know and may follow, or at least pay lip service to, the numerous rules and advice we get – eat right, exercise, limit alcohol intake etc. In the data-processing world, doing backups may have the same status with many clients. For some, it may be "something your systems guy sets up for you, so you don't worry about it". For others it may be "don't really need it, I have a Raid 5 setup and the redundant hard drives will keep me safe" (or insert the technology of your choice). It may be easy to pay lip service to backup processing and that may bring disastrous results.

This Tips & Tricks will cover the critical importance of backups and provide a few useful tips.

Passport regularly has reports of critical lost data from failed hardware, failed backups or malware making both PBS and customer data inaccessible. Sometimes we can help and sometimes not, and unfortunately, we hear about some businesses losing multiple years of data from this kind of catastrophic event.

Some recent reports:

> "I'm living this scenario with a customer right now … Their IT folks spun up a new virtual server for them back in 2020 …. They were hit with malware and had assumed the IT folks … had this server being backed up with the others. No such thing."
> "My customer was backing up their PBS to their London office, however, the ransomware found that network path and total data loss occurred."

What can we say that might be new or useful about this, given that everyone knows they should be doing backups?

Design your Backup System

Don't treat backups as something just for the techs or your networks guys. Be proactive and co-design your backup system with them, giving it the same attention as you would your accounting system. As a guide for gauging the design issues, a rule of thumb could be to ask and answer the question "how much time and effort will I suffer if I have to rebuild data starting from …" be it 4 hours ago, a day ago, several days ago. Answering that question based on the number of people who will be involved, what data is absolutely crucial and must be restored including manual re-entry of data, and including estimates of the time to locate the source documents and recreate the data, will provide a guide as to what is the net worth of each day or hour's worth of data i.e., the cost of reproducing your data prior to the event. Factoring in the inconvenience of gathering the source documents after they have been filed or archived and re-establishing your starting point is an implicit additional cost.

These estimates should produce a reasonable assessment of risk and imply a return on investment for the backup system. A perfect solution is likely beyond the budgets of most companies because it would require continuous and secure backups and no interruption of computer services even while a fault was happening. This would require multiple levels of redundancy and automated fail-over when a fault happens.
Here are a few issues to be considered and options:

- Precisely what data should be backed up
  You can be selective if you have concerns about backup times and volumes of data or you can simply backup everything. For example, if you create archive companies to hold old data that is not being changed, you might be able to save having to back up gigs worth of data that will not change over weeks or months.

- Incremental backups
  Having incremental backups- i.e., only backing up changed data is a good scheme for situations in which keeping data volumes minimal is useful. This is true for example, for collections of individual documents which are essentially independent of each other, and which can be updated without reference to the other documents. This means if document A changes on Wednesday, it will be backed, but if document B wasn't changed till Friday, it won't be on the backup till then.

  However, when a backup is needed it is almost *always a time of some stress and anxiety if not panic* and having the most recent data spread between multiple incremental backups somewhat complicates getting the right version of the data all restored properly. This is especially important for accounting data because if, for example, you restore the AR Open Items back to a certain point back in time you also must also restore the equivalent version of the billing history files as well as the GL Distributions or GL Transactions. And the list goes on. In other words, data consistency and integrity are absolutely critical for accounting systems and that dictates the accounting system data likely should be backed up as a unit. So incremental backups at least for the accounting system may not be the best option but can be useful for documents like spread sheets and PDF's.

- Frequency of backups
  The frequency of backups is an important issue. Simple backups like a single daily backup that is kept for say a week, may suffice and certainly keeps things simple since there will only be 7 copies kept at any time before the first one is recycled. However more frequent and/or more extensive retention times may be desirable. For example, if you have large amounts of data fed into the system automatically e.g., using the PBS Data Import Manager, having the backup done daily may not suffice. Twice a day or even continuous backups may be available depending on the nature of the software you choose.

  The requirement here is for reasonably good backup and cost-effective protection. For most businesses, a once-a-day backup is actually reasonable in terms of the down-side loss of data and balances against a modest investment for the backup equipment and services.

- Retention
  Retention - the number of backups and how long you keep them is key. While a week's worth of daily backups will cover most situations where a complete restore is needed; it may be worth considering setting aside a backup once a week for a month or more so that coverage goes back that far. This becomes useful in cases where a document is accidentally deleted, and its absence is not discovered for several weeks. Similarly, data being purged might not be discovered within a simple one-week period. With only daily backups for a week, that document or those purged items would be unrecoverable.

  In addition to having weekly backups, having "specialized" backups which are kept indefinitely are a good idea. For example, a year-end backup done just before all the current accounts are cycled back to become last-year accounts (i.e., just before you press the button(s) to close the year) may be a good idea to regain a financial position for reporting during an audit. It would also be useful in payroll to record your position for W2s and before closing your payroll year. If your year-end is non-calendar, then this reasoning can be extended to run a special 1099 or payroll year-end backup that captures the accounting positions as of 12/31 and then a second year-end for your fiscal close say in June. Another circumstance for a special backup is to record the pre-change position of the company prior to some major transition such as a purchase of the company or some fundamental changes to operations, reporting or chief personnel.

  To this list of special backups, you could add an extra backup method. For example, assuming you are using a cloud daily backup you could purchase a large enough terabyte drive to cover one or two complete backups done periodically e.g., once a week. This would back up the backup and is a rather inexpensive additional safety precaution. For example, when the lights go out suddenly and that crashes your system, your cloud-based backups may also not be available immediately once power comes on. However, if you have one or two machines working, your terabyte backup will be available. This might mean being able to

get that contract out in time and could make the difference between winning or failing to get that $100K contract.

Location of your backups

Cloud, network or removable drive backups – where is the backup data to be stored?

Part of the design of your backups is where the backups are located and how easy is it to restore a hard-drive or a file from a specific date/specific backup. In many cases, your tech company will have a preference based on their experience. A strong network and internet-oriented company may prefer a cloud-based backup, whereas a hardware-oriented company may have more experience and comfort with a NAS (network accessed storage) or equivalent.

For most situations, providing the software and hardware that are aligned with current standards may not be a big issue providing it a can do the things you need in your design. However, it is important to get answers for questions like "How easy is it for me to restore a whole disk drive" or "the whole accounting system" or "just one file". "How long will this take"? "Can I do it by myself or do I have to give my techs a call to get it done? "And," Can you guarantee me 'n' hours or less response time to do this"?

The second issue related to location of backups comes from the increasing sophistication of malware. Current malware, once it is on a network, can spread in minutes if not seconds. If you are hit with a Ransomware attack, typically your action steps may be to pay the ransom or else immediately disconnect your business from the internet and completely rebuild your system from fresh untainted sources. If your backups are on the same network e.g., on a NAS, then the backups most likely are infected and of no help in restoring the system. These situations require that a backup be available offline. In the tape backups days, people could take their "Friday backup tape" home with them and this offsite backup would satisfy this requirement. Nowadays, cloud-based backups generally will be OK, but backups accessible through your network could be a problem – more to discuss with your techs. The potential solution here is to have a removable device such as a USB-3 multi-terabyte drive which is used periodically e.g., once a week, to provide a backup that has no permanent connection to your system ensuring safer remedies against these attacks.

Testing your backups

All of the above relates to the design elements of your backup system. As important, or possibly more important, is the ongoing element – testing. Many of the horror stories we hear about relate not so much to the design but to the fact that some time after the backup system was started, it failed and no one realized that the failure had taken place. For the first few weeks after start-up, people will generally be interested enough in checking on the backup system but ongoing diligence gets boring even when there is a daily email sent to one or two people giving the statistics of last night's backups. (These emails are often a good idea if the software supports this function.)

However, bad things do happen to good systems. For example, consider: a particular partition containing the accounting system is backed up as an image file. A new major upgrade to the accounting system needs more space or is there is a move to PBS SQL, and a new partition is set aside for it for the new version. The old partition is kept for some time for historical purposes and people move to the new version of the accounting system on the new partition. Through an oversight the backup system is not changed to include the new partition – and no errors are posted since the backup is still finding the old partition and backing it up. Six months later a serious crash in the accounting system leaves them without the backups for the last six months.

A second quick example: a carefully designed backup system includes a daily email sent to a system supervisor confirming the backup. That supervisor moves on to another job, the emails continue to get sent, but not to the new supervisor. And then the system fails but no one notices.

Bottom line, it is imperative to periodically review *and test* your backup technology and methods. Whether this is monthly, quarterly or annually will depend on a number of factors:

-how easily can you see the date/time stamps of the backup files?
-are confirming emails being sent?
-are logs being generated giving files and bytes backed up?

Even with all of these being checked and looking normal, ***actually doing a restore*** of the data is important. For two reasons. First, it gives you direct and positive feedback your backups are working and that *they can be successfully restored.* Secondly, it keeps the issue of the importance of backups top of mind, so this issue doesn't get overlooked and your backup fails without anyone noticing.