Five Keys to Preventing Data Corruption in Storage Environments

The lifeblood of a corporation is in the information that it generates and stores. Due to the increasing amount of data and information that an organization must protect, robust computer systems are essential for survival. The failure of these systems, whether due to problems with hardware, attacks from external influences, viruses or a poorly written application can cause information to become corrupt. This type of destruction can render the information useless. Without safeguards in place, the financial health of the corporation is in jeopardy. Measures need to be developed by the IT department and implemented regularly to prevent this scenario from occurring.

Perform Regular Backups

A regular backup routine is a critical component of any effort that prevents the corruption of data. During this process, the method used to create an image or copy of the data should only be done once at a specific time. The data should be written with read-only access to prevent any accidental overwriting of the information. Once the backup operation has completed, verify that the data is intact and cannot be modified. This also presents the perfect opportunity to verify that the media used is of high quality. Perform validation testing to ensure that the data stored on the backup media is in fact usable.

Choose Backup Media Carefully

One of the disadvantages of using portable electronic media such as tapes or DVD is that they are prone to experience wear and degradation over time. Even the highest quality media will cause some data corruption in storage environments because of this fact. As such, a policy to establish how long data backups should be maintained needs to be implemented. For more critical data, multiple backup routines should be in place. A good rule of thumb is that one piece of media should not include large amounts of data. Sets of media should be created to have some functionality in relation to the data and the system in which they back up. In the worst case scenario that corruption occurs on these media sets, an entire system

will not be affected.

A better alternative for backup media would be external hard drives that are connected locally to the system. The rationale behind this is that the operating system has the built-in capability to detect problems during the write process. If an area on the hard disk is not usable for recording information, the system will mark it as such. It will continue with the next available space. Once the backup procedure has been completed, these external drives can be removed and stored in a safe location. The downside is the cost of this type of storage media can be prohibitive for large-scale data backup operations.

Utilizing a combination of optical or magnetic media and external hard drives can provide a happy medium. The most critical data and information would be safeguarded on the hard drives. Data that can be easily recovered or reintroduced into the system would be worth the risk of using DVD or tape backup. A major factor to keep in mind for preventing data corruption in storage environments is to have a manageable plan to restore the system with minimal risk. It may be cost effective for a company to lose a day or weeks worth of data if the savings of using optical or magnetic media outweigh the potential for loss.

When selecting media in the forms of DVD or tape, the cost of the equipment reveals much about its quality. Media that comes in bulk for discount prices are prone to more errors and have more instances of failure. If this is the chosen route for performing backups, then adequately testing the backup image before new transactions are conducted is highly recommended. Again, it all boils down to how much risk a company is willing to endure in the case of corruption. Higher quality media does come with a higher price tag, but the advantages far outweigh the costs.

Take Precautions

When it comes time to restore data from backup media, certain precautions should be implemented before the operation begins. Creating a valid return point is highly recommended in case data corruption in storage environments occur during the restore process. This will allow the ability to roll back to the previously created point before the restore procedure began. If data errors do occur when

trying to restore media from backup, don't immediately give up on the process. Have some robust tools available that will allow rebuilding the image. There are many applications that have the ability to restructure data that has been damaged.

Try Several Tools to Recover Corrupt Data

Recovery tools can piece together segments of data to restore corrupted image backups provided that enough information is readable. Backup processes will sometimes add extra information to the data known as parity bits. This helps to restructure an incomplete sequence of data. Other smart technology can restore missing bits and bytes of data by determining the most likely value for the corrupt bit. Don't give up after one failed attempt; a few different restore applications should be tried. Where one application may be unable to rebuild a corrupted image, a different software solution may specialize in fixing the problem.

Verify, Verify, Verify

As with the completion of a backup operation, verify that the restore procedure worked correctly. Take some extra measures to ensure that no data corruption in server environments took place before allowing the system to go live. Double check all of the log files to detect any unusual activity. Perform some spot checking on the data that was re-introduced to the system. If anything looks suspicious, follow up and make sure that all hardware and software systems are operating as expected. Do not proceed with regular business activity until 100% confidence has been realized. One small error could result in wide scale corruption problems.