



Home Entertainment Made Simple

Threats against System Availability & Catastrophic Data Loss on Media Centers

A Look at Available Solutions

By Steven W. Cheung

About the Author: Steven Cheung is a co-founder of VidaBox LLC, an innovative manufacturer of premium media center / home theater PC systems and helped standardize VidaSafe™ data protection onto all VidaBox™ media centers, dramatically increasing media center uptime and system availability.

If you're concerned about maintaining maximum uptime on a media center, or worried about hard drive failures destroying your valuable music CD, digital pictures, DVD, video, and other digital media collections, a new standard in storage technology may be the solution you are looking for.

The Need for Data Protection

For years, people have typically stored digital content on standard computer hard drives. This allowed users to have instant access to hundreds & thousands of different songs, pictures, DVDs, videos, and files. However, little thought is usually given to uptime, availability, data redundancy, or backups. Common threats to data, such as viruses, malware, and spyware can be usually rid of with a suite of utilities without other data on the hard drive. While damaging, these threats are usually not catastrophic and are manageable with tolerable loss of data and downtime.

On the other end of the spectrum, total system failures and losses of data, such as those from hard drive failure (the most destructive & common cause of total failure), are considered to be "rare" and thus, usually not guarded against. However, this often results in the devastating loss of family pictures, camcorder videos, entire music collections, and other invaluable media. Data recovery services are sometimes used in the hopes of recovering portions of the missing media, but the cost and time involved are astronomical with no guarantee of success. In the end, the system is still not available for use.



All data stored onto hard drives are susceptible to loss. Conventional recovery methods are expensive while success is not guaranteed.

To prevent catastrophic data loss, most users usually do backups of their data on a regular basis. This is a prudent measure, as one would always have an "image" of their data. However, most users do not have the equipment or know-how necessary to do a truly complete disk image. So, when the hard drive fails, not only will they lose new data since their last backup, they will also lose the use of their system until replacement parts come in. Furthermore, unless the user is technically-savvy, s/he will have to wait for a technician to replace the failed hard drive, reinstall the operating system along with all the programs, and finally, restore the data from the backup. This process to restore system usability, from start to finish, can still take weeks.

Backups using optical or magnetic media are impractical for media centers due to storage limitations.

Network-attached storage for a backup of 500GB can take as long as 41 hours.

Backups are only as good as the media it is stored on. Most users never test their backups, not knowing if it will fail when they are needed most.

However, on a media center, a backup process is not practical. Typical optical media (DVD±R) can only store 4.7GB, whereas typical media centers can store from 500GB upwards to 3.5TB+ of data. Magnetic media and external hard drive storage have much higher storage capacities, but the time required to backup, for example, 500GB of data can be as long as 41 hours^[1] - totally impractical for a daily, "up-to-the-minute" backup. Furthermore, backups do not improve the uptime or availability of the media center, which has to be on 24/7.

Worse of all, backup processes assume that the backup media is fully functional. Some users who copy their data onto magnetic or optical media find that there are errors on their backup from to repeated use when it comes time for a restore. Thus, conventional hard drive storage technology is simply not good enough for the cutting-edge demands of today's media center systems. A newer level of protection is required, not only for system availability and uptime, but also data protection.

What to Look for in Media Center System Protection

Finding the right type of protection for your media center may require some investigation, so here are a few things to look for:

- **System Uptime & Availability Protection**

A media center must be able to record TV shows at any time of the day or night, so it must be as reliable as possible. Thus, a media center should feature a fault-tolerant protection system where no data loss or downtime should occur, even if a hard drive has failed.

- **System Restorability**

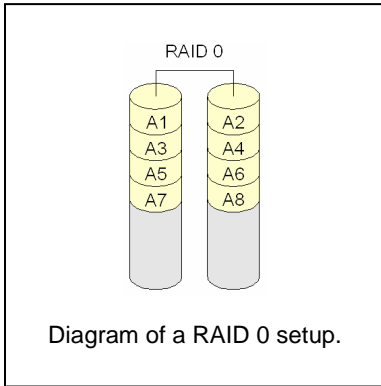
In the event of a virus, malware, or spyware infiltration, the operating system may have to be "wiped clean" and reinstalled. The system should allow reformatting of the operating system drive without any loss of data to maximize restoration speed and reduce downtime.

- **Easy-to-use & Transparent to the User**

A variety of products are available to attain high reliability & simplified system restorability. However, many of them are either very expensive and cost-prohibitive, or they're affordable but complicated to use and require constant maintenance and interaction. The ideal solution should be pre-installed and built into the system, run "in the background", and be completely transparent to the user. A balance between protection costs and ease-of-use must also be reached.

What Solutions Are Available

To maximize system uptime and availability, RAID (Redundant Array of Independent Disks) is becoming the new standard in hard drive failure and data protection. There are a variety of RAID levels commonly used in media centers, some of which are explained below.

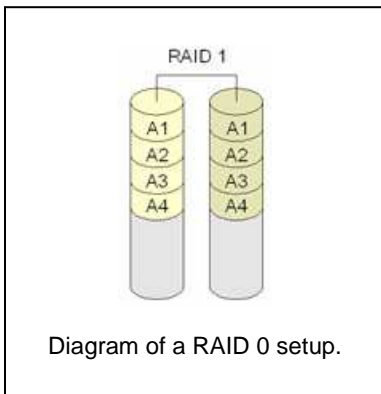


• **RAID 0**^[2]

A RAID 0 (also known as a stripe set or striped volume) array splits data evenly across two or more disks, but it stores no parity information for redundancy.

RAID 0 is normally used to increase performance, and is commonly used as a way to create a small number of large virtual disks out of a large number of small physical ones. Writing and reading throughout performance is increased.

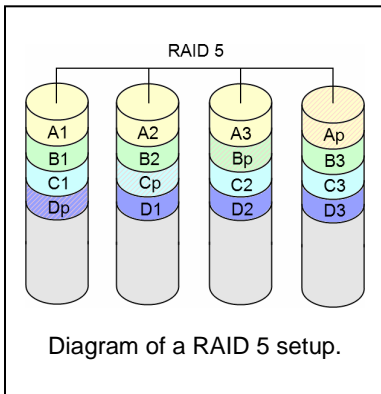
This RAID level should be avoided, as it provides no actual data protection.



• **RAID 1**^[3]

A RAID 1 (also known as mirroring) creates an exact copy of a set of data on two or more disks. This is useful when read performance is more important than data capacity. A classic RAID 1 mirrored pair contains two disks, which increases reliability exponentially over a single disk. Since each disk contains a complete copy of the data, and can be addressed independently, ordinary wear-and-tear reliability is raised by the power of the number of self-contained copies.

However, because of the amount of storage space required for the redundant data, a system's total storage capacity will be limited to half of its maximum potential, creating unnecessarily high storage costs. Another solution might be more appropriate.



• **RAID 5**^[4]

A RAID 5 the most popular of the RAID levels, uses block-level striping with parity data distributed across all member disks. This is a balanced solution between adjoining independent disks as a larger disk (RAID 0) and complete mirroring (RAID 1) and allows a low cost for redundancy.

How RAID 5 works

Unlike the complete 1:1 mirroring in RAID 1, redundancy is achieved by the use of parity blocks. Like RAID 0, the throughput for reading data on the RAID 5 array is improved since the data being sought is stored on a number of independent disks.

In the event where a single drive in the array fails, data blocks and a parity block from the working drives can be combined to reconstruct the missing data.

Given the diagram on the left, we assume A1 = 00000111, A2 = 00000101, and A3 = 00000000. Ap, a parity check generated by applying Exclusive Disjunction (XOR) on the A1, A2, and A3 values, will then equal 00000010.

If the second drive fails, where A2 will no longer be accessible, the A2 value can be reconstructed by applying XOR on the A1, A3, and Ap values:

$$A1 \text{ (XOR) } A3 \text{ (XOR) } Ap = 00000101 \text{ (A2)}.$$

Exclusive disjunction, also known as exclusive or and symbolized by **XOR**, is a logical operation on two operands that results in a logical value of true (1) if and only if one of the operands, but not both, has a value of true (1).

RAID 5 does not protect against viruses, spyware, or other malware.

Thus, one can conclude that RAID 5 is almost a requirement for any media center system. However, RAID still does not protect against other common sources of system problems such as:

- Viruses
- Spyware
- Malware

To protect against these different threats, a different solution must be found, which is discussed below.

Logically Isolated Operating System & Storage Drives

Operating System Restores usually require drive reformatting causing complete data loss on that drive.

Even with a suite of anti-virus and anti-spyware software, a media center may still be infected on a rare occasion. While traditional software can usually restore and "heal" damaged files, sometimes the only way to be sure that a virus or other malware has been destroyed is to completely reformat the operating system's drive. On most systems, everything - the operating system, music, TV shows, DVDs, and other media files - is stored on one single drive. Reformatting the drive will result in complete data loss!

To prevent this hurdle, the operating system and storage drives must be logically isolated. Thus, even if a virus strikes the operating system and renders it completely useless, the drive can simply be wiped clean and its software reinstalled without any loss of data on the isolated storage drive.

Self-operating & Self-maintaining protection systems

Automated & self-maintaining protection systems require no user input and help assure minimal downtime.

Even if a media center is completely protected against hard drive failures and the operating system are easily restored, user maintenance and interaction still may be required. This is impractical for a media center, since the only interface usually used is a simple remote, whereas a PC or file server can have a keyboard and mouse connected. Furthermore, users of media centers

Thus, a system should be self-optimizing. Tasks such as defragmentation, automated shell interface memory purging, & anti-spyware updates should all be running automatically at a low-use time (e.g. at night) without any user interaction.

Pre-installed/Built-in Protection

It is much more time and cost-effective to purchase a media center with a pre-installed/built-in protection system rather than retrofit an older system.

Most media centers do not have these key protection components, but retrofitting and installing these features into a pre-existing system will be an expensive & time-consuming task.

If a media center has not been purchased yet, look for a model that already includes these components to ensure system reliability and dependability.

Where to Go From Here

This paper merely addresses the data protection features required in a media center. If you are looking for a media center that includes all of these features plus more, we offer VidaBox premium media centers that include VidaSafe™ Data Protection technology.

VidaSafe™ Technology
*automatically defends against
data loss in cases of:*

- *Hard Drive Failures*
- *System Restores due to virus
or spyware attack*

VidaSafe™ data protection technology is the first trademarked system that defends against all of the aforementioned threats to a media center. It works in the background, built-in as a part of the basic input-output system. Every VidaSafe™-protected drive features RAID 5 protection for optimal uptime, assuring system availability even in the event of a hard drive failure. The operating system and data storage drives are logically separated, making data loss during complete system reinstalls a thing of the past. In concert with self-updating & self-running maintenance software, this array of carefully engineered and designed protection components achieve impressive uptimes of 99%+^[5] and system availability.

To find out how to get VidaSafe™ technology, featured exclusively on the VidaBox™, contact us today at (516) 730-7500 or visit our website at <http://www.vidabox.com>

References:

[1] The Buffalo TeraStation Home Server takes 24:56 to backup 5GB of data. Simply multiply by 100 to obtain value for 500GB.
http://reviews.cnet.com/Ximeta_NetDisk_Portable_500GB/4505-6407_7-32017036.html

[2], [3], [4] RAID descriptions and diagrams courtesy of Wikipedia at:
<http://en.wikipedia.org/wiki/RAID>

[5] VidaBox LLC Internal Testing and Performance Lab Data - VidaBox systems require 4 mins of reboot time on average for system updates, plus reboots initiated by users. 99%+ figure allows for 3.36 hours or less of actual downtime. Actual calculated uptime test rate is 99.9% (better than advertised).

Copyright © 2006 VidaBox LLC.

No part of this document may be distributed, reproduced, or posted without the express written consent of VidaBox LLC.