



Data Protection and Recovery

Introduction

In this fast-paced world there is one thing most computer users have in common. We have all lost data at one time or another. For the lucky ones, this is not a painful experience, just one of inconvenience. Unfortunately for others, the data loss is impacting because the lost data was irreplaceable and valuable. If they are fortunate, their lost data is personal and not owned by their employer. One thing is certain. Most people become very diligent about protecting their data after suffering a major data loss.

Years of experience have taught us the importance of buying insurance for our house or our car. But unlike property or car insurance, data protection strategies have not been around that long. People are just now learning the hard lessons about the importance of protecting the digital property that they own and value. Just like buying insurance, putting together an effective data protection plan is usually not at the top of most people's list of things to do. Regardless, it is important that everyone using information in digital form devise some way of protecting that data to ensure it will be there when needed. Compounding the need for data protection is society's shift to the widespread use of digital media in everyday life, such as storing digital photographs on a computer instead of storing physical photographs in photo albums. Now all types of personal and business information are vulnerable in ways they never were before the advent of computers.

The good news today is that there is an easy and automated way to protect data by making copies to a secure location and providing status reports that the data was copied successfully. There are many types of data storage solutions available and choosing the right one is as important as the decision you make to start protecting your data. This white paper will examine the different types of technologies, explore their characteristics, and determine how effective they are at protecting your data from all types of threats. After you have read this document, you will have information that will allow you to choose the right technology to effectively protect your important data.

Ways Data Can Be Lost

As you think about how to protect your data, it's important to understand the different ways in which data can be lost. A successful data protection strategy takes into account all of the ways in which data loss occurs. Not all will apply to you but it's important that you consider each to determine the impact on your important data.

Event	Impact
Device Failure	This can be as simple as a bad spot on a disk where your file is located or your entire disk drive could fail. When this happens you generally have to wipe and reinstall your entire operating system from the files which were protected.
Equipment Failure	This is similar to a device failure but is more complex. For instance, if you're using a RAID-based storage system, there might be a failure in the equipment that affects all the drives resulting in the loss of all the data. This also includes a failure like memory corruption within your computer causing information to be written incorrectly. This case would require the defective equipment be replaced and the information recovered.
Data Corruption	Data corruption occurs because of failure of the software to correctly store the information or it can accidentally overwrite existing information.
User Error	User error is the most common reason for data loss. If you have been using personal computers for many years, you may remember the command "delete *.*" Before the Windows interface it was quite common to go and delete files using that command and not understand the global impact it had on all the files in the directory. Today with the Windows environment, deleting a file is not a catastrophic event as long as we recognize the fact that we deleted it before we empty the recycle bin.
Site Destruction	Site destruction is a localized event such as fire or flood that holds the destruction to a localized area. Recovery from a site destruction event is more complicated as the equipment and the site must be replaced.
Viruses	Viruses are something which we all experience and, due to the intervention of virus scanning tools, we tend to feel less threatened when we find them on our computers. When you consider how virus tools detect and eliminate viruses you might not remain so comfortable. In order for the global virus database to be updated, someone must be infected and the viral engineers must have enough data to identify and characterize the virus before they can update the database. This means that hundreds to thousands of people can be affected by the virus before a detection method can be developed and the virus eliminated. If you're lucky, the virus will only be one of inconvenience and annoyance; however, it could be a virus of destruction and your data could be permanently lost. These types of viruses can be quite devious.
Hackers	Hackers are another way in which data can be lost. Most of the hacking we hear about involves lawless individuals breaking into a system looking for private information but what we don't hear about is hackers breaking into a system and sabotaging the computers and data. Any company that experiences such a breach is reluctant to share that information with the public, fearing the effect on its public image or its market valuation. Only when the breach involves private and confidential information of customers are companies required by law to disclose the breach publicly. Hacking has become a tool of organized crime and terrorists since the effect on the value of a company allows these individuals to make money on the fall of its stock price.
Natural Disasters	Natural disasters are the worst because of the scope and size of the affected area. Not only is the equipment lost, but the facilities are destroyed and personnel unavailable. Recovering from a natural disaster is not as easy as simply relocating to a new building and installing your equipment. The process is much more complicated as a new location far away from the natural disaster must be found and the infrastructure must be rebuilt from the ground up. Most companies in areas that are vulnerable to natural disasters have disaster recovery plans in place. This recovery usually involves staging computer equipment in a city far from the disaster zone and programming the computers there so they can be brought online as quickly as possible after the disaster. They also have alternative trained personnel who can arrive during an emergency and get the company back on their feet again.

Data Protection Basics

Having discussed the things that can destroy your data, it is time to look at some of the basics of data protection. It is important to have an understanding of these basic concepts before you choose the type of technology you'll use to protect your data.

Time to Protect (also known as the backup window)

This is the amount of time needed for your device to make a copy of your data and verify that it's been done properly. Different technologies take different times to complete this process. The protection process can also be quite resource intensive and may be an activity you choose not to do while using your computer. In the storage world the time needed to back up your data is known as the backup window and represents an impact because of application unavailability while the data is being backed up. Typically, the backup window opens at a time where it would generate the least amount of inconvenience and closes prior to the time when most users would need that information.

Time to Recover – Recovery Time Objective

Time to recover or restore your information is an important consideration when you are choosing the right technology for your data protection strategy. Some technologies provide the ability to restore your lost information instantly while others may take minutes or hours to restore. If you need to be back online immediately after a data loss, then you need to choose a technology that provides the fastest recovery time. However, the technology that provides the fastest recovery does not necessarily provide the best protection.

Recovery Point Objective

Knowing what the state will be when restored involves knowing when the data was backed up so that any subsequent changes can be identified. The recovery point is defined as a known state so any additional changes can be applied to bring the data up to the current state of when the data loss occurred.

Level of Protection

The level of protection for each technology must be weighed carefully when making your selection. For instance, if you must recover data immediately, you may choose one technology to do the immediate recovery. But because of its limited ability to protect against all types of data loss, a second layer of protection may have to be

implemented. This is typically referred to as a multi-level data protection and recovery strategy and involves multiple types of technologies to allow you recover data faster as well as protect against all types of data loss

Point-In-Time Copies

Multiple point-in-time copies are important because you may want to have more than one version of your file protected. There may be situations in which data is corrupted and you're not aware of the corruption for many days. If only one copy of your data is made, then your last copy (and therefore the only copy) will also be corrupted. By creating multiple point-in-time copies you have the ability to go back in time to a copy which was not affected by the data corruption and recover your data.

Data Protection Technology Choices

As mentioned earlier, there are several technologies available for data protection. They are generally broken into two categories: fixed storage solutions using disk technology and removable storage solutions using tape technology.

Disk-Based Data Protection

Typically, disk-based storage solutions can be comprised of a single disk drive or multiple disks, as in the case of a RAID-based system. Multiple RAID-based systems can also be used in a data protection strategy. Some of the techniques used by a fixed storage solution are disk-based backups, mirroring, snapshots, and replication. A disk-based protection is not removable and therefore cannot be rotated off site for increased protection.

Since disk-based solutions are not removable they cannot protect against all forms of disaster unless an expensive remote replication solution is installed. The remote replication solution includes replicating the storage system at a remote site and communication links (usually fiber optic cables) to transfer the replicated data to the remote site. These implementations do offer some level of protection against device failures, equipment failures, site destruction, and natural disasters, yet remain vulnerable to viral attacks and hackers if extensive safeguards are not employed. The only way to assure the ultimate protection is by having the data on a removable media and storing it in a secure location.

Tape Based -Data Protection

Tape-based backup is a classic solution focused on tape drives and libraries. Tape is the most cost effective solution from a cost-per-megabyte perspective, and

it is the only traditional solution other than optical that offers removable storage suitable for offsite storage. However, the speed of recovery for tape solutions can be slower than snapshots, clones, and mirrors.

Which Solution is Best for You?

The dilemma is which protection strategy should you use? Based on everything we have discussed, you can see that if your greatest need is for fast recovery, disk-based storage solutions may be your best choice. But since disk-based solutions do not protect against all forms of data destruction, you would also need to implement tape-based solutions. The good news is that there is now a solution that combines the best of disk and tape - RDX® removable disk technology from Boulder, CO-based ProStor Systems. This storage solution allows you to have the fast access and recovery speed of disk combined with the removability of tape.

Enterprise-Class RDX Systems Replace Tape for Backup & Archive

ProStor Systems has developed the industry's first removable disk technology that offers data backup and archive to removable disk storage with enterprise-class reliability. The company's RDX products combine and improve upon all of the best characteristics of today's tape and hard disk drives, and at an affordable price. Their high-performance, enterprise-class data protection, transportability, affordability and scalability meet all backup, archiving and disaster recovery requirements for servers, networks and professional workstations.

Disk to Removable Disk for Backup & Archive

ProStor's RDX system offers a better solution than tape, using a rugged, reliable removable disk cartridge. The RDX cartridge can be used to back up over 125 GB of data in an hour, retrieve files in milliseconds, and safely archive data for over a decade. The RDX system, which is 10 times more reliable at retrieving archived data than tape drives, offers the only removable disk solution to actually replace tape in all backup and archival applications ranging from small enterprises to data centers.

Conclusion

As stated earlier, it is not a matter of if but when you will lose some or all of your valuable computer data. By developing a data protection strategy today, you will be taking out one of the smartest insurance policies money can buy. Choose the storage system that offers you the most comprehensive coverage for the most reasonable price. You'll reap the benefits of your data protection strategy now and for many years to come.