

How to Protect SMB Data

By: Randy Kerns, CTO —ProStor Systems, Boulder, CO

The need for protecting data is universal – whether a small to mid-size business, the largest enterprise data center, or an individual. The recognition of the value of information and the impact of data loss has reached the point where repeating it is no longer required. The issue now has turned to how to protect the data.

For small to mid-size businesses, there are several options but some basis must be established for defining what characterizes a small to mid-size business and the considerations that are specific for them. Understanding these characteristics will help in sorting the available data protection options into a more likely set of choices that will meet the required needs.

Some classifications segment businesses based on the number of employees or the amount of revenue. For small to mid-size business, the most commonly used numbers in size and revenue are shown in the following table.

Designation	Employees	Revenue
Mid-size business	100 to 1000	\$26M to \$100M
Small business	10 to 100	\$1 M to \$25M

More important than the number of employees or revenue in defining the size of businesses regarding data protection is how they deal with storage. The amount of storage capacity is not what defines whether a business fits into the small to mid-size business category. Quantity of data stored has significant variability depending on the type of industry and the regulations required in that industry. Using a capacity number can distort the perception of a business. What is important is how these businesses administer storage of their data. The capacity demand increases are similar across businesses in the same industry regardless of the size. What is different is the means of dealing with meeting the capacity demands. Typically, small to mid-size businesses will have an IT staff that does not include a storage specialist. A systems administrator will handle storage as an added task in providing the systems support for applications. With this diffusion of responsibility, data protection is usually perceived to be something that must be simple to implement and administer. In addition, the demands are usually immediate because of the lack of time to invest in implementing a storage strategy.

The data protection options must be viewed with the requirements of the small to mid-sized business – simplicity in deployment and administration, cost of the system to be installed, and longevity of the technology to protect the investment and minimize additional effort over the long term. The different options all warrant some consideration but many can be quickly discounted based on their ability to meet the small to mid-size business requirements.

Data Protection Options

Each of the options involves applying some technology in the data storage area to protect data. There is not a single definition of what data protection means however. In general, the protection in the context for this discussion means protection against loss of data access.

Replication of data with Online Storage Systems

One option is to make copies of data to additional disk storage that is currently online. Making an online copy would provide for relatively fast backup and recovery but at the risk of having the data unavailable due to being co-located and not physically protected as with removable media. In addition, procedures must make multiple copies of the data to ensure corruption in the primary copy is not propagated to the backup copy. The extra physical capacity required represents a significant additional cost for storage as well as increased operational expenses. This is true regardless of the disk system type or connection – whether it is block storage or file-based using NAS or whether the storage is RAID protected or not.

A remote replication solution where the online system is at a physically remote site would provide the physical protection but is cost prohibitive for any small to mid-size business.

Copies of data to External USB Disks

Replicating data to external USB disks provides some measure of protection by allowing data to be replicated to another disk system that is external to the normal operating environment. A problem with this approach is that cyclic or periodic backups with retention of prior versions in some rotation is difficult with a limited number of external USB disks. In addition, external USB drives are not ruggedized to be handled as removable media so offsite storage is impractical.

Copies of data to flash memory drives

Copying data to flash memory devices is a rapid transfer method used in the way that floppy disks were used in the past. Using flash drives for backup of business systems with ever-growing capacities is problematic because of the number required based on capacity and the relative cost. Data protection using flash memory devices is usually limited to specific files and normally used for interchange.

Remote Service Providers

Using a remote service provider involves sending data over a network to another system where the small to mid-size business data is stored by the provider. The price charged is based on the amount of data stored and the frequency of transfers of data. Recovery involves retrieving the data over a network from the remote site. Small to mid-size businesses typically find the expense of network connections that would provide enough bandwidth to retrieve data when it is needed most in a restoration to be prohibitive. In addition, the restoration process still resides with the customer and some degree of functioning system will be required to retrieve the data.

Optical Storage Systems

Using optical storage for data protection provides the removability that is needed by small to mid-sized businesses for disaster protection. Optical devices include UDO, MO, and the ubiquitous DVD and CD drives. The problems presented with optical devices for many business applications has been the capacity of the individual devices has not kept up with the growing capacity of disk technology, the performance is below other competing technologies, and the durability of the media in handling with removability has been an issue.

Tape Storage Systems

Long the media of choice for protecting data, tape devices that are in the price range of small to mid-sized businesses have not matched the capacity increases seen by disk devices. In addition, the reliability when viewed as measured by the success of restores has not improved enough to meet customer expectations. Consequently, in the target markets, the use of tape for data protection is not a focus area for most IT professionals. Tape does provide the removability expected in the market and allows for media to be cyclically used for generational data.

Removable Disk Systems

Removable disk systems represent the newest technology to be utilized for data protection. Removable disks can be thought of as similar to tape in that a removable media is used in a drive mechanism. Only in this case, the cartridge that is the removable media contains a disk device. Using disk drives as the removable media allows for the backup device to capitalize on the same technology investments and follows the same development curve as the primary storage medium. The advantage of using disk which is a random access device over a sequential access device gives greater performance in restoring data when it is needed most. With a design that can withstand the handling expected for removable media and a repeated use model that far exceeds tape cartridges, removable disks provide both reliability and long-term economic advantage. The key to the removable disk capability is the design of the drive and of the cartridge – the characteristics of those will be reflected in the ruggedness, cost, performance, and the ability to utilize newer disks of greater capacity.

A summary of the data protection option follows:

Data Protection Option	Features	Issues
Online Storage	Copies of data to another disk. Fast backup and restores.	No removable media. Expensive
External USB drives	Copies to another disk attached to USB port.	Does not allow cyclical backups.
Flash Memory Devices	Fast memory transfers	Not suited to cyclical backups. Expensive at large capacities.
Remote Service Providers	Data replicated offsite to a provider storage system	Restoration may require faster bandwidth than is affordable by SMB.
Optical Storage Systems	Backup to removable media.	Capacity and performance not in step with disk. Durability of media issue.
Tape Storage Systems	Traditional backup to removable media.	Reliability and technology pace compared to disk. Drive costs and number of usage cycles of media are expensive
Removable Disk System	Fast and reliable backup to removable media. Rugged cartridges that follow disk technology curve.	

Small to Mid-Sized Business Data Protection Practices

There are many different strategies employed for data protection at small to mid-sized businesses. Some are very specific to the circumstances of an individual company. Others are just variations of ways that data protection may be done differently. There is not necessarily a 'best practices' template because of the different circumstances but there are a few general guidelines that provide assurances that the information of a company is being protected.

Part of data protection includes archival where data that is unlikely to be needed in day-to-day activity is moved to another type of device where it is protected and can be recalled when needed. By archiving the data, it is removed from the normal backup requirements and the primary storage space that it would have occupied is available for usage to satisfy other capacity demands.

The primary data protection practice for small to mid-sized businesses is to back data up to a removable media device. The backups are typically done on a periodic basis to establish a known point called the recovery point objective if a restore is required. According to business practices, the backups are usually cyclic where on average four copies of the removable media are rotated through the backup. For the physical protection from disaster, usually a complete set of backup media is taken offsite weekly. Backups may be done as complete backups or some form of incremental where only changed data is backed up. Incremental backups are a concession to the amount of time a backup requires where the complexity of recovery is traded off against the availability of the data for operation. This 'backup window' is as much a product of the speed of the devices as anything and the use of faster backup devices may change the tradeoff decision.

A practice that is often overlooked or left undone is that of testing backups. On a regular basis a backup needs to be restored to provide some measure of assurance that the data protection being done will work when it is most needed. Without some testing of backups, there may be a latent problem that will only be discovered at the worst possible time.

Backing up data is with the general assumption that the recovery operation will be successful when needed. If the experience has been that some percentage of recoveries fail, usually the data protection practice is enhanced to create more than one copy at periodic times. This extra backup is an additional insurance policy that has come about due to some problems that occurred with unreadable tapes. With the use of removable disk technology, this extra backup should be greatly reduced.

The Big Picture

The need for protecting valuable information for a business is well established. The fact that there are several options now should cause a re-examination by small to mid-sized businesses to inventory their process for protecting information, understand the probability of successful recovery, and look at the ongoing costs both in capital expenses over time and operational expenses. Just doing that evaluation can lead to a greater confidence in continuing business operations after some impacting event.

The evaluation is not as complicated as it may sound. Asking questions, looking at the common practices and comparing against current operations, and understanding the dynamics of adding more storage to meet the capacity demands and the implications on data protection is enough to cause a realization that some changes may be required. With that realization, the value of the options for data protection and how they meet the demands will become more apparent.

Not examining the current state of data protection and making plans for changes that occur may put data at risk. Not choosing the right backup technology may also put data at risk and may be ultimately very costly.

Conclusion

A small to mid-size business has the same business requirements for data protection as a large enterprise. The capacity growth demands are proportional and the information is of no less value. Attention must be paid to providing data protection that meets business needs.

With the recent addition of removable disk technology as a more reliable, cost effective and higher performance solution for data protection, small to mid-size businesses need to re-examine their needs and consider deploying removable disk as the technology to continue with in the future.

ProStor Systems has developed the RDX removable disk system which provides enterprise-class capabilities but yet is targeted at the small to mid-size businesses. It brings the technology and roadmap of disk to a removable cartridge that has a long life without having to upgrade to a new version in a few years. The RDX fulfills the SMB customer needs for a data protection solution.