



White Paper:
**Ten Steps to Safeguard
Business Data**

Your business has distinct needs that differ from either consumers or larger businesses. Sales and customer service are your main priorities, and while IT functions are important, you may not have staff dedicated to them. In that case you may choose to outsource part of your IT needs. Even if your business does have dedicated IT staff, they probably concentrate on business productivity and administration, with responsibilities ranging from implementation of new systems—such as ERP / business management—to desktop support. As a result, tasks such as data backup, security and retention often do not get the attention they deserve, especially given the impact they may have if not performed adequately.

What should you do to protect your data if your resources are limited?

1. Make sure you can recover your data.

Of course, the main reason you back up your data is so you can recover it. But backing up and recovering data efficiently and reliably requires sophisticated technology and up-to-date hardware. While some backup approaches use simplified methods to reduce the burden of the backups, they can make recovery difficult or impossible. For example, the most common approach used with tape backup is to perform periodic full backups, and more frequent incremental backups between them. If a full backup is done weekly, the files you need to recover may be on the last of six incremental backup tapes. To recover your data, you would need to first restore the last full backup and then each of the incremental backups in order. If any one of the backups failed, you wouldn't be able to restore your data. This can occur when an operator forgets to remove a tape from the prior backup before starting the next backup and thus overwrites the prior one. When that happens the data from all subsequent backup jobs won't be accessible.

Make certain your backup approach is foolproof and reliable.

2. Safeguard your business from a major disaster.

Hurricanes, floods, tornados, earthquakes and other natural disasters can threaten the viability of your businesses if you aren't prepared. The best way to thwart this is to routinely back up to an off-site data center. Anything less is playing Russian roulette. That data center should be both adequately remote and certified secure so you are absolutely certain of recovering from a disaster.

3. Determine how much data loss is acceptable.

The next safeguarding step is to determine how much data—and which types—can be lost without seriously affecting your business. When you back up your data periodically the consequence of a simple disk failure will very likely be the loss of all data since the last time a backup was conducted.

Examples: Point-of-sale or order-entry databases, online transaction databases, or other servers may hold critical data. For some businesses, e-mail may also be critical. If you back up data more frequently, you reduce the amount of potential lost data and allow users to resume business faster. Determining how often you need to do this in order to retain crucial data is referred to as your recovery point objective or RPO. Of course, more backups—especially if performed manually—may require more diligence and entail higher costs.

Consider a solution that automates backups according the schedule you require.

4. Decide how long can you be without your data.

Next, calculate how long you can operate without your data. In other words, when you experience a disaster, how long can you tolerate operating without access to it?

Consider a baseline of 24 to 48 hours. Sort your data into three categories. The first is important data, but you will be satisfied if it takes longer than 48 hours to recover it. The second category is data you will definitely need within 25 to 48 hours. Third is data you need in less than 24 hours. This is referred to as the time to return-to-operations or RTO.

5. Resolve which backup solution best matches your resources.

Keeping your business successful means doing more with less. Your priorities are sales and service, not the details of data management. This means you may want to outsource functions, such as data protection and management, which don't directly add value to your business. On the other hand, you may consider it cost-effective to have your staff manage the data protection effort. Ideally, the solution you use will make setup and administration easy, and restoring files fast and intuitive (the saying "set-it and forget it" comes to mind). The best data protection solution lets you choose how you implement it.

6. Get the flexibility to outsource.

A key point in step 5 above was the ability to hand over management of your data protection to a local consultant. If you do so, be sure he has the tools to set up, monitor and administer everything about your data backup and recovery from his remote location. A further key: It's quite possible that as your company grows, you'll want to take your data protection back in-house. So, look for a solution that makes this possible seamlessly.

7. Be sure your backups are secure and comply with regulations.

The keys: end-to-end encryption and certified data centers. Look for a solution that encrypts your data during transmission and in storage. Get a vendor who moves your backups to an offsite data center that's SAS 70 Level II certified.

If you need to comply with regulations such as SOX, GLBA, or HIPPA—and who doesn't anymore—make sure the vendor you select helps you conform to your industry-specific requirements. Ask if they have customers in your industry and are willing to refer you to them.

8. Ensure you can back up the type of systems and applications you use.

It may sound obvious, but make sure you can back up and recover all the data types you use or are likely to use on the platforms in your environment. Every vendor can back up the standard array of documents, databases and images. But can they do so when your employees have those files open? Your most important data is likely to be in use when you want to perform backups. If you can't back up open files, important data won't be safeguarded or you will need to stand down to perform backups.

Perhaps more importantly, you may have specific applications that require specialized support including Microsoft Exchange, Microsoft SQL Server, and VMware. Also make sure your solution includes support for the Microsoft Windows family of desktop and server operating systems, and consider the need for other platforms too, including Linux.

9. Consider which backup technology is best for your business.

While a backup to a CD, DVD or local hard drive can protect you against a physical disk failure, it won't help you in the case of a major disaster. Tape backup is also widely used; however, tapes are prone to operational errors and have low recovery success rates. Using any of these local backup media also fails to reliably protect against catastrophic failure because it is difficult to get the data adequately far enough offsite to safeguard against a local or regional catastrophe. (See step 2.)

Today many businesses choose online, disk-to-disk backup and recovery because it makes possible all the steps in this guide.

10. Find a good vendor.

Do what it takes to be clear about what you're getting in a data protection system. Talk to lots of vendors. Ask them about the steps listed above. If you want to really dig deep, request case studies and contact the customers cited in them. They'll be upbeat for the most part. But ask them about things that went awry, and how they felt about the support they got. If they're candid, they'll share some of their past pain. The keys are at the ends of their stories. Listen for something like, "They wouldn't give up until my problem was solved."

That's the kind of thing you hear about i365 EVault Data Protection solutions. Over 20,000 customers trust their expertise to safeguard critical data. With EVault you rest assured your data is secure and readily accessible. They treat your data as if it were their own. And since they're backed by Seagate, you can count on the people of EVault to be there for you.