Storage Guardian

White Paper

7 Critical Characteristics

to Demand from Your Remote Backup Service

The biggest danger businesses have with remote backup services is lack of knowledge in what to look for.

There are literally hundreds of companies offering this service because they see it as an easy way to make a quick buck. But not all service providers are created equal and you absolutely want to make sure you choose a good, reliable vendor or you'll get burned with hidden fees, unexpected "gotchas," or with the horrible discovery that your data wasn't actually backed up properly, leaving you high and dry when you need it most.

If your remote backup provider doesn't meet all 7 of these points, then you'd be crazy to trust them to store your data:

1 Military-level security, data transfer, and data storage.

This is fairly obvious; you want to make sure the company housing your data is actually secure. After all, we are talking about your financial information, client data, and other sensitive information about your company. Never trust your data to anyone that doesn't have the following security measures in place:

a. Ask your service provider if they are HIPAA, Sarbanes-Oxley, Gram-Leach-Bliley, and SEC NASD compliant. These are government regulations that dictate how organizations with highly sensitive data (like banks and doctor's offices) handle, store, and transfer their data. If you are a medical or financial institution, you are required by law to work only with vendors who meet these stringent requirements. But even if you are NOT an organization that falls under one of these regulations, you still want to choose a provider who is because it's a good sign that they have high-level security measures in place.

b. Make sure the physical location where the data is stored is secure. Ask your service provider if they have an ID system, video surveillance, and some type of card key system to allow only authorized personnel to enter the site.

c. Make sure the data transfer is encrypted with SSL protocols to prevent a hacker from accessing the data while it's being transferred.

2 Multiple data centers that are geographically dispersed.

Anyone versed in data security knows the best way to avoid loss is to build redundancy into your operations. All that means is that your remote backup service should store multiple copies of your data in more than one location. That way, if a terrorist attack or natural disaster destroys one of their locations, they have backups of your backup in a different city where the disaster did not strike.

3 Demand the ability to receive overnight copies of your data on DVD or some other data storage device.

If your entire network gets wiped out, you do NOT want Internet download to be your only option for recovering the data because it could take days or weeks. Therefore, you should only work with a remote backup provider that will provide overnight copies of your data via some physical storage device.

4 On that same token, ask your service provider if you have the option of having your initial backup performed through hard copy.

Again, trying to transfer that amount of data online could take days or weeks. If you have a large amount of data to backup, it would be faster and more convenient to send it to them on DVD.

5 Make sure your data can be restored to a different computer than the one it was backed up from.

Amazingly, some backups can only be restored to the same computer they came from. If the original computer was burned in a fire, stolen, or destroyed in a flood, you're left without a backup.

6 Demand daily status reports of your backup.

All backup services should send you a daily e-mail to verify if your backup actually ran AND to report failures or problems. The more professional providers should also allow you to notify more than one person (like a technician or your IT person) in addition to yourself.

7 Demand help from a qualified technician.

Many online backup services are "self-serve." This allows them to provide a cheaper service to you. BUT if you don't set your system to back up correctly, the money you will save will be insignificant compared to the losses you'll suffer. At the very least, ask your service provider to walk you through the steps on the phone or to check your settings to make sure you did the setup properly.