DP Solutions
Problem Solved.

FREE REPORT

It's Time to Re-think How You're Protecting Your Data

If your data is important to your business and you cannot afford to have your operations halted for days – even weeks – due to data loss or corruption, then you need to read this report. The report outlines why businesses need to re-assess their approach to backup and disaster recovery (BDR), what the BDR landscape looks like today, and lastly what you should be looking for in an effective data protection solution.

In this Report, You'll Discover:

- The CRITICAL role that technology plays within an organization, despite what many owners may think.
- Why thinking of disaster recovery simply as an insurance policy to be used in the case of an extreme event can be DETRIMENTAL to your business operations.
- How to determine the Return on Investment (ROI) of a Disaster Recovery Solution.
- What remote or offsite backups are, and why EVERY business should have them in place.
- Seven critical characteristics you should DEMAND from any remote backup service.
- What you can expect to pay for an effective managed backup and Disaster Recovery solution.

Most business owners understand that data backup and IT disaster recovery is a way to protect their key information and technology systems, allowing their business to function in the event of a disaster or outage. This concept is not new and businesses have many options for protection nowadays.

However, even with all of the known risks to not protecting their data, a lot of companies are still without a system for disaster recovery (DR). Unfortunately, businesses often treat DR as something they will only worry about when, and if, they are faced with an emergency. This is a detrimental mistake. According to the Institute for Business and Home Safety, an estimated 25% of small businesses never re-open their doors after a disaster. Lack of planning to protect and recover data, plays no small part in this scary statistic.

SO WHY ARE BUSINESSES PUTTING THEMSELVES AT RISK?

Oftentimes, it has to do with the way in which organizations view IT as a whole. Many business owners regard IT as a necessary evil that they have to deal with in order to operate functionally.. They fear that vendors and consultants are trying to sell them more IT hardware and infrastructure than they really need. As a result, they approach purchasing new technology with a high degree of suspicion.

Yet, the reality is that many organizations are run on their technology infrastructure. For instance, businesses rely on email to communicate with vendors and customers; their accounting is all done on applications that reside on a server; and they often manage customer interactions on a Customer Relationship Management (CRM) tool or some other line of business application. Therefore, business owners must ask themselves how essential those applications are to running their organization.

BUSINESSES NEED TO CHANGE THE WAY THEY THINK ABOUT DISASTER RECOVERY

Many businesses think of Disaster Recovery as a high tech insurance policy that will only be useful if an unlikely, catastrophic event occurs. There are two MAJOR PROBLEMS with this ideology:

1. Viewing DR as a solution solely in case of an extreme event (i.e. hurricane, tornado, fire, etc.) ignores the most common incidents that cause IT outages such as loss of power, loss of Internet connectivity and hardware failures. These events are not uncommon at all, but can have the same effect of causing downtime and an interruption in business that a fire might have.

2. Viewing DR as an insurance policy is problematic. Fire insurance, for example, will provide money to rebuild an office space after a fire, but it does not prevent interruption of day-to-day business operations. However, a quality DR Solution will keep critical technologies running while the emergency is happening, and as steps are being taken to recover.

5 STEPS TO DETERMINE THE ROI OF A DR SOLUTION

To understand the Return on Investment (ROI) of your DR Solution, you must identify the following:

1. Each critical process that your technology powers.
2. What critical processes can be done manually and what processes require a technology-based system.
3. How time consuming the manual processes are (for a day, for a week, etc.).
4. The cost of running transactions manually (employee productivity, hourly wages, etc.).
5. The cost of lost opportunities if customers can't reach you by email.

Business owners need to shift their thinking and understand that a "disaster" can often be as common as someone tripping over a plug, or spilling water causing a power outage. A proactive DR plan allows a business to continue operations DURING a disaster, not just recover lost data afterwards.

Once you understand the value of IT services to your business, you can make informed decisions about your IT infrastructure. In the case of DR, business owners and key stakeholders need to identify the cost of losing their technology-based services and invest in the correct IT hardware, services and support to avoid or minimize downtime. The value of any given system should determine how much you spend to ensure its availability or uptime.

REMOTE BACKUPS: WHAT THEY ARE AND WHY EVERY BUSINESS SHOULD HAVE THEM IN PLACE

If you are like most business owners, you have been smart enough to at least set up a tape backup. But know this:

HALF OF ALL TAPE BACKUPS WILL FAIL TO RECOVER LOST DATA! ARE YOU WILLING TO TAKE THOSE ODDS?

Most people don't realize that at least 50% of tape drives will fail in a data recovery attempt*. But what's really dangerous is that most companies don't realize this happened until it's too late. While you should maintain a local backup of your data, a tape backup will not offer adequate protection.

To completely protect your data and guarantee that you could restore it after a major disaster, you MUST maintain an up-to-date copy of your data offsite, in a high-security facility.

Subsequently, remote backup, also called offsite backup, is a service that allows you to maintain a secure copy of your data in a different location than your office.

Usually remote backup is done automatically via the Internet to a high-security facility. There is no question that every business owner should have an offsite copy of their data. However, there ARE big differences among remote backup services and it's critical to choose the best solution and a provider you trust.

*Source: http://datamountain.com/services/livevault/tapes-fail/

THE 7 CRITICAL CHARACTERISTICS TO LOOK FOR IN 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 options for a remote backup service. However, not all solutions are created equal. You want to make sure you choose a good, reliable vendor. If the proper steps are not taken, you may run the risk of being burned with hidden fees, unexpected "gotchas," or discover that your data wasn't actually backed up properly.

THE 7 "MUST-HAVES" TO LOOK FOR WHEN CHOOSING YOUR REMOTE BACKUP SERVICE:

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 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. 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.

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

2. **Offers multiple data centers that are geographically dispersed.** Depending on your level of risk tolerance, multiple copies of your data stored in more than one location might be necessary. Even if you only need your data backed up to one location currently, your provider should be able to offer you the option to have your information backed up to more than one data center should your needs change in the future.

3. **The ability to perform "Full Metal" restores offsite.** If your entire network gets wiped out, you do NOT want an Internet download to be your only option for recovering the data, because it could take days or weeks. You should only work with a remote backup provider that can restore your server, in its entirety, both locally and offsite to a virtual server. If the original server was burned in a fire, stolen, or destroyed in a flood, you're left without a backup. You want to be sure your backups can be restored to a virtual version of the server, so no hardware is required to keep things running.

4. **Data can be restored to a different server than the one it was backed up from.** Amazingly, some backups can only be restored to the same server they came from. **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 a large 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 your provider on DVD.

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

6. **Regular tests and restores.** One of the most critical characteristics is finding a company that will perform regular test restores to check your backup and make sure the data is recoverable. **You do not want to wait until your data has been wiped out to test your backup.** If your data is very sensitive and you cannot afford to lose it, then test restores should be done monthly. If your situation is a little less critical, then quarterly test restores are sufficient. Any number of things can cause your backup to become corrupt. By testing it monthly, you'll sleep easier at night knowing you have a good, solid copy of your data available in the event of an unforeseen disaster or emergency.

7. **Managed by qualified technicians.** Many online backup services are "self-serve." This allows the provider to offer a cheaper service to you. BEWARE…YOU GET WHAT YOU PAY FOR! Look for a managed services provider (MSP) that has multiple, qualified engineers on staff. These engineers should know how to setup the solution, manage the backups, and be available 24x7 for any tech support issues that may come up. It may cost a little more up front, but it's nothing compared to the losses you'll suffer if you happen to make a mistake by using a self-managed service.

   The average amount a typical small business (3 to 5 servers and 1500 GB of storage) can expect to pay for any decent, fully managed backup and disaster recovery solution is around $1500 to $2500/month. If you go much lower than that, your provider is most likely cutting some corners.

WANT TO KNOW FOR SURE IF YOUR DATA BACKUP IS TRULY KEEPING YOUR DATA SECURE?

OUR FREE DATA PROTECTION ASSESSMENT WILL REVEAL THE TRUTH…

Learn just how secure and reliable your data backup really is with our free, no obligation data protection assessment.

At no charge, one of our backup specialists will evaluate the current state of your backups, including:

- Your current data protection, including backup and restore procedures, tape rotations and maintenance schedule to see if your data's security is jeopardized.
- Procedures for storage and transportation of data. Many people don't realize they can easily damage their disks (and thereby corrupt their data) by improperly caring for their storage devices.
- Your network backup to ensure they are accurately backing up all of the critical files and information you would NEVER want to lose.

After we have gathered all the information, we'll create an easy-to-understand report outlining our findings, explaining in plain English where your risks are. Depending on what we discover, we'll either give you a clean bill of health or reveal gaps in your data backup that could prove disastrous. If it's appropriate, we'll provide you with an action plan for further securing your data.

Visit info.dpsolutions.com/protect to get your Free Data Protection Assessment today!