“The 9 Ugliest Mistakes Made with Data Backup and How to Avoid Them”

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 and act on the information shared. This report will outline the most commonly made, costly mistakes that most small business owners make with their data backups.

You’ll Discover:

- What remote, offsite, or managed backups are, and why EVERY business should have them in place.
- Why ONE copy of your precious data is simply not enough!
- How Disaster Recovery Plans will give you a false sense of security.
- The best, most effective way to TEST your data backup strategy.
- The ultimate scorecard you should use to select a data backup provider.
- Frightening Trends and Cases you should consider.
- Other common and costly mistakes that are routinely made when backing up critical data…
Have you ever lost an hour of work on your computer?

Now imagine if you lost days or weeks of work – or imagine losing your client database, financial records, and all of the work files your company has ever produced or compiled.

Imagine what would happen if your network went down for days and you couldn’t access e-mail or the information on your PC. How devastating would that be?

Or, what if a major storm, flood, or fire destroyed your office and all of your files? Or if a virus wiped out your server…do you have an emergency recovery plan in place that you feel confident in?

How quickly do you think you could recover, if at all?

If you do not have good answers to the above questions or a rock-solid disaster recovery plan in place, you are quite literally playing Russian roulette with your business. With the number of threats constantly growing, it’s not a matter of if you will have a problem, but rather a matter of when.

But That Could Never Happen To Me!
(And Other Lies Business Owners Like To Believe About Their Businesses…)

After working with over 700 small and mid-size businesses in the Capital Region, we found that 6 out of 10 businesses will experience some type of major network or technology disaster that will end up costing them between $9,000 and $60,000 in repairs and restoration costs on average.

That doesn’t even include lost productivity, sales, reputation and client goodwill that can be damaged when a company can’t operate or fulfill on its promises due to technical problems.

While it may be difficult to determine the actual financial impact data loss would have on your business, you can’t deny the fact that it would have a major negative effect.
“But I Already Back Up My Data,” You Say…

If you are like most business owners, you’ve been smart enough to set up a data backup. But know this:

Most Data Backups Suffer From At Least One of the Following 9 Ugly Mistakes!!

1. **The Scope of the Backup is Incomplete**
   It is very common to see a data backup that has very little strategic thought behind it. Evidence of this mistake presents itself in the form of:
   - Important Data, Applications, or Systems that are NOT included in the backup job(s).
   - All Data, Applications and Systems are backed up the exact same way – there are no priorities.
   - The time it takes to ACTUALLY recover lost or corrupt data is much longer than expected.
   - The point in time in which you are ACTUALLY able to restore to is too far in the past (I want to recover yesterday’s information, but I am only able to recover last month’s information!)

   Avoid this mistake by classifying and prioritizing the data, applications and systems that need to be backed up. A Business Impact Analysis will identify critical sets of data and define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). This allows you to implement a backup job that supports lightning fast restore times for CRITICAL information.

2. **Backups are Not Completed Automatically**
   All too often we see backup jobs that require a person to manually start the backup. The process to start the backup job is usually very simple, like clicking a button. However – PEOPLE FORGET TO DO IT!! Backup jobs should always be automated. Automation eliminates human error or neglect and yields a much better chance of having a successful backup when you need it most.
3. There is Only ONE Copy of the Backup
   There should always be more than one copy of your data backup. For critical systems, we recommend having THREE copies – for less critical systems, we recommend having TWO copies. The logic is simple, what happens if your data backup is lost, deleted or becomes corrupt? If you need to restore from backup, is it more comforting to have only one recovery source, or is it more comforting to have a few recovery sources?

4. Backups are Not Monitored for Success
   So many businesses have a “set it and forget it” mentality about their data backup jobs. NO ONE EVER CHECKS TO SEE IF THE BACKUPS ARE SUCCESSFUL!! For this reason it is important that your backup jobs are monitored very closely and if there are any errors (and there will be from time to time) that cause a backup job to fail – YOU NEED TO BE NOTIFIED. There are many systems that are available to provide monitoring and alerting services for backup jobs. You must keep a close eye on your backups; otherwise you will find yourself in a very bad situation one day.

5. Backups are Not Kept Offsite
   It is very common for data backups to be kept onsite, in the same physical location of the systems that are being backed up. While this practice is acceptable for some types of systems failures (hardware failure, software corruption, etc.), it is a terrible idea for other types of failures. For example, if your building floods or burns – and your servers are severely damaged – do you think the backup media that was located right next to those servers will also be damaged? YES, IT WILL BE! For this reason, it is important to keep at least one copy of your data backups offsite, at a different physical location.

6. There is Insufficient Capacity for Backups
   The backup job is 400GB, but your backup tape or drive is only 300GB. Capacity issues have a tendency to create sloppy and incomplete backup jobs. It is imperative that your backup media be sized and provisioned to not only support your current backup needs, but also allow for some element of growth over time. A simple Capacity Planning exercise conducted by a qualified technician is incredibly important to your overall backup strategy.
7. There is No Documented Disaster Recovery Plan
   Often we see backup jobs that are working very well. Critical data is being backed up at regular intervals which support organizational RTO and RPO requirements. Then, disaster strikes. There is a power outage that fries the server, the network room floods, the building burns down, etc. A backup job is only successful if data can be easily and quickly recovered. You need to have a recovery procedure documented! Typically this is in the form of a Disaster Recovery (DR) Plan. The plan should include important procedural steps involved in recovering lost data and should also indicate who is responsible for performing those steps once a disaster is declared. If you choose to not have a documented DR Plan then recovering from a disaster will be chaotic and frustrating at best!

8. There is No Process to Add or Remove Items from the Backup Scope
   As new servers, applications and data repositories are added to your computing environment – they also need to be added to your backup job(s). It is very important to have a documented Data Backup Policy that outlines the process for adding or deleting components of the data backup job(s). Without a policy, new systems may or may not be integrated into the backup job(s) effectively and old systems may never get removed. Once you have a great data backup job, you want it to stay great. This requires governance and oversight typically provided by good policies and procedures.

9. Backups are Not Tested; People are Not Trained
   Data backup job(s) absolutely, positively need to be tested AT LEAST ONCE A YEAR – if not more frequently. A true test is the only way to verify that critical information can be restored if needed. More importantly, people (employees, vendors, etc.) should all be educated on the restore process, especially if they play a critical role in restoring lost or corrupted data. A common and effective way to provide this training is by conducting routine Table Top exercises where DR scenarios are presented to the recovery team and they have an opportunity to respond – without creating any service disruptions.
Frightening Trends, Cases, and Questions You Should Consider:

- Tape drives fail on average at 100%; that means ALL tape drives fail at some point and do NOT offer complete protection for your data if a natural disaster, fire, or terrorist attack destroys your office and everything in it. Business owners who were hit by hurricanes like Katrina learned a hard lesson about keeping remote backups of their data.

- 93% of companies that lost their data for 10 days or more filed for bankruptcy within one year of the disaster, and 50% filed for bankruptcy immediately. (Source: National Archives & Records Administration in Washington.)

- 20% of small to medium businesses will suffer a major disaster causing loss of critical data every 5 years. (Source: Richmond House Group)

- This year, 40% of small to medium businesses that manage their own network and use the Internet for more than e-mail will have their network accessed by a hacker, and more than 50% won’t even know they were attacked. (Source: Gartner Group)

- About 70% of business people have experienced (or will experience) data loss due to accidental deletion, disk or system failure, viruses, fire or some other disaster (Source: Carbonite, an online backup service)

- The first reaction of employees who lose their data is to try to recover the lost data themselves by using recovery software or either restarting or unplugging their computer — steps that can make later data recovery impossible. (Source: 2005 global survey by Minneapolis-based Ontrack Data Recovery)
The Ultimate Scorecard to Critique
a Data Backup Provider

The biggest danger businesses have with backup services is lack of knowledge in what to look for in a Data Backup Provider.

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 Data Backup Provider doesn’t meet all of these points, then you’d be crazy to trust them to store your data:

1. They conduct a Business Impact Analysis (BIA)
2. They write a custom Data Backup Policy
3. They write a custom Disaster Recovery Plan
4. They complete a Capacity Planning Exercise
5. They INSIST on having at least TWO copies of your backup
6. They monitor your backup jobs for errors and failures
7. They provide alerting and notification
8. They maintain, support and fix your backup jobs
9. They offer free recovery services
10. They INSIST on testing your data backups
11. They INSIST on providing training
12. They have documented Service Level Agreements (SLAs) backed by 100% money back guarantee
13. They offer a no risk cancellation policy – there is never a penalty to cancel services.

Courtesy Scorecard Provided on the Next Page…..
<table>
<thead>
<tr>
<th>13 Questions You MUST Ask Before Hiring Anyone to Manage your Data Backups</th>
<th>Company A</th>
<th>Company B</th>
<th>Company C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do they conduct a Business Impact Analysis to determine RTO and RPOs?</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Do they write a custom Data Backup Policy?</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Do they write a custom Disaster Recovery Plan?</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Do they complete a Capacity Planning Exercise?</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Do they INSIST on having more than one copy of your backup?</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Do they monitor your backup jobs for errors and failures?</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Do they provide alerting and notification mechanisms?</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Do they maintain, support and fix backup jobs?</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Do they offer FREE data recovery services?</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Do they INSIST on testing your data backups?</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Do they INSIST on providing Table Top training exercises?</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Do they have documented SLAs?</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Do they stand behind a 100% money back guarantee?</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Do they offer a no risk, cancellation policy where there is no penalty, ever, to cancel services?</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

**Your Choice…**

**Want To Know For Sure If Your Data Backup Is Actually Working?**
Our Free Data Backup Assessment Will Reveal the Truth…

As a prospective new client, we’d like to extend a “get to know us” offer of a Free Data Backup Assessment. We don’t normally give away free services at TAG Solutions because if we did, we’d go out of business. But since your company meets our strict selection criteria, we thought this would be a great way to introduce our services to a few new clients.

At no charge, a data backup specialist will come on site and…

- Audit your current data protection including backup and restore procedures, tape rotations and maintenance schedule to see if there is anything jeopardizing your precious information.

- Document actual Recovery Time and Recovery Point Objectives (RTO and RPOs).

- Check your network backup to make sure they are accurately backing up all of the critical files and information you would NEVER want to lose.

- Verify that backup media has sufficient capacity for routine backup jobs to successfully complete.

- Discuss current data backup needs and explain in plain English where your risks are. We know everyone has a different level of risk tolerance, and we want to make sure all the risks you’re taking with your data are by choice not because of miscommunication or accident.

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 with our TAG Vault managed data backup service.

Naturally, we don’t expect everyone to become a client, but we do expect a small percentage to hire us to protect their most valuable asset—corporate data—and possibly even become loyal clients.
You are Under No Obligation to Do or Buy Anything When You Say “Yes” to a Free Data Backup Assessment

We also want to be very clear that there are no expectations on our part for you to do or buy anything when you take us up on our offer.

As a matter of fact, we guarantee that you won’t have to deal with a pushy, arrogant salesperson because we don’t appreciate heavy sales pressure any more than you do.

However, we cannot extend this offer forever because time and staff limitations simply won’t allow it. In order to secure your Free Data Security Analysis for your company, you must respond to this offer by May 13, 2015. Spots ARE limited so act today. We regretfully will have to withdraw this offer and make it available for someone else if you are unable to respond on time.

Claim your FREE Assessment now by simply filling out the request form on this page – or – download a request form here, that can be mailed or faxed back to us – or – Call us at 1-844-340-3520 – or – email your request to databackup@tagsolutions.com.