

2012

DATA PROTECTION ESSENTIALS FOR NON-PROFIT AND BUSINESS EXECUTIVES

Revealing the most common problems that plague non-profits and businesses causing data loss.

This monthly briefing provides executives with the knowledge needed to make good decisions when implementing a data recovery, data backup, and disaster recovery strategy.

**Executive Briefing for March 2012
By BeckITSystems, Inc.**



DATA PROTECTION ESSENTIALS FOR NON-PROFIT AND BUSINESS EXECUTIVES

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 Will Discover:

- What remote, offsite, or managed backups are, and why EVERY non-profit and business should have them in place.
- 7 critical characteristics you should absolutely demand from any remote backup service; do NOT trust your data to anyone who does not meet these criteria.
- Where tape backups fail and give you a false sense of security.
- Frightening trends, cases, and questions every executive should know and consider regarding data security.
- The single most important thing to look for in a remote backup service provider. ®

BeckITSystems
Inc.

**From the Desk of: Ed Becker, President
BeckITSystems, Inc.**

To: Non-Profit and Business Executives

Dear Colleague,

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 organization 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 Believe About Their Businesses...)

After working with over 700 non-profits and businesses, we have found that 6 out of 10 businesses without proper data recovery technology and strategies 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, lost sales, and lost client goodwill that can happen when an organization cannot 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 organization, you cannot deny the fact that it would have a 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 tape backup or some other type of backup program. But know this:

The average failure rate for a tape backup is 100% - ALL tape backups fail at some point in time. Other organizations with other types of backup experience and average of 2 weeks of down time getting to a recovery, on average!

Incredible, isn’t it? Most people don’t realize that ALL tape drives fail. But what’s really dangerous is that most organizations don’t *realize* it happened until it’s too late.

That’s why history is riddled with stories of organizations losing millions of dollars worth of data. In almost every case, these organizations had some type of backup system in place, but were sickened to find out it wasn’t working when they needed it most, or that it required extraordinary effort and expense to recover from the problem.

While you should maintain a local backup of your data, a tape backup will NOT offer you protection if...

1. Your tape drive malfunctions rendering it useless and making it impossible to restore your data. IMPORTANT: It is *very* common for a tape drive to malfunction without giving any warning signs.
2. Your office (and everything in it) gets destroyed by a fire, flood, hurricane, tornado, or other natural disaster.
3. The physical tapes you are backing your data up to become corrupted due to heat or mishandling.
4. A virus spoils the data stored on the tape drive. Some of the more aggressive viruses not only corrupt the data, but they don’t allow anyone to access the data on the drive.

5. Someone in your office accidentally formats the tape, erasing everything on it.
6. Theft – a disgruntled employee intentionally erases everything, or a thief breaks in and steals ALL of your equipment.
7. A faulty sprinkler system “waters” all of your electronic equipment.

Bottom line: You do NOT want to find out your backup was not working when you need it most.

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. Executives who lead organizations that were hit by hurricanes like Katrina learned a hard lesson about storing backups of their data in an off-site location more than 500 miles away from their location.
- 93% of organizations 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 organizations (1-200 employees) 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 organizations 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*)

Remote Backups: What They Are and Why EVERY Organization Should Have Them

The **ONLY** way to completely protect your data and guarantee that you could restore it all after a major disaster is by maintaining an up-to-date copy of your data in at least one high-security facility far from your location.

Remote backups, also called off-site backups, online backups, or managed backups, is a service that allows you to maintain a secure copy of your data in a different location more than 500 miles from your office.

Usually this type of backup is done automatically via the Internet to a high-security facility. There is no question that every executive should have an offsite copy of their organization's data; however, there ARE big differences among remote backup services and it's critical that you choose a good provider or you could end up paying a lot of money only to discover that recovering your data — the very reason why you set up remote backups in the first place — is not an easy, fast, or simple job.

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 be 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 criteria, then we recommend against trusting them with 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 organization. Never trust your data to anyone that does not 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 is 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 AES protocols to prevent access to 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 to recover after your Internet service is available. Therefore, you should only work with a remote backup

provider that will provide overnight copies of your data via some physical storage device.

4. **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 by a secure delivery service on a computer hard drive.
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, damaged beyond repair, stolen, or destroyed in a flood, you are left without a backup.
6. **Demand continuous monitoring of your backup services with regular written status reports.** All backup services should provide monitoring 24x7 of your backup status and verify that your data was properly stored. Any failures should be alerted in the monitoring services AND failures or problems quickly fixed. Monthly status reports of the backup should be provided to you in writing.
7. **Demand help from a qualified technician.** Many online backup services are “self-serve.” This allows them to provide a cheaper service to you; HOWEVER, if you do not set your system to back up correctly, the money you will save will be insignificant compared to the losses you’ll suffer.

The Single Most Important Thing to Look For When Choosing a Remote Backup Service

While the above checks are important, one of the most critical characteristics – and one that is often overlooked -- is finding a company that will do **regular test restores** to check your backup and make sure the data can quickly be recovered.

You do not want to wait until your data has been wiped out to test your backup; yet that is exactly what most people do – and they pay for it dearly.

If your data is important and you cannot afford to lose it, then test restores should be performed at least monthly. If your situation is a little less critical, then quarterly test restores may be sufficient.

Any number of things can cause your backup to become corrupt. By testing it monthly, you will sleep a lot easier at night knowing you have a good, solid copy of your data available in the event of an unforeseen disaster or emergency.

To Know For Sure That Your Data Backup Is Keeping Your Data Secure, Request Our Free Technology Security Analysis To Know the Truth...

With spring and summer storms just around the corner, BeckITSystems is offering non-profits and businesses with 20 to 200 employees a “get to know us” offer of a Free Data Security Audit. We do not normally give away free services from BeckITSystems, Inc. because if we did, we would go out of business. But in this down economy, it is our contribution to the success and survivability of organizations that meet the requirements. We also believe this could be a great way to introduce our services to a few new clients.

At no charge, a security specialist will come to your location and...

- Audit your current data protection including backup and restore procedures, tape rotations and maintenance schedule to see if there is anything jeopardizing your data's security.
- Review procedures for storage and transportation of data. Many people don't realize they damage their disks (and thereby corrupt their data) by improperly caring for their storage devices.
- 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.
- Present a simple and easy to understand chart that will detail the makeup of your data, including the age and type of files you are backing up. Why should you care? Because many organizations unknowingly use valuable computer storage to back up their employees' personal MP3 files and movies.

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

Depending on what we discover, we will either give you a clean bill of health or reveal gaps in your data backup that should be sealed. If it is appropriate, we will provide you with an action plan for further securing your data with our Hassle Free IT Continuous Data Backup Program.

Naturally, I don't expect everyone to become a client, but I do expect a small percentage to hire us to protect their most valuable asset--corporate data--and possibly even become loyal clients.



BeckITSystems[®]
Inc.

I Don't Need a Free Security Analysis Because My Network Guy Has it Covered...

Maybe you don't feel as though you have an urgent problem that needs to be fixed immediately. Maybe you think your data is perfectly safe. Many of our current clients felt their data was safe until it became necessary for them to RESTORE THEIR DATA.

Unfortunately, that is when most organizations "test" their data backup and restore solution. We are helping organizations like yours AVOID embarrassing and extremely costly data catastrophes like these **REAL LIFE STORIES**:

A diversified company in Loudoun County, VA, which was NOT a BeckITSystems' client, thought their data was backed up to tape each night. They had an IT guy that was responsible for this and they spent thousands of dollars on the appropriate tapes, tape drive, and software to protect all their critical data. As you can imagine, the company was devastated when they found that all their data was deleted by a trusted employee AND the tapes were all blank because the employee created backup jobs that ran but did not backup data.

Flash forward three weeks, **\$162,000 in data recovery and auditor fees later**, all the data was successfully restored. The company said that the worst part of the whole experience is thinking you are doing all the right things spending money on solutions that APPEAR to be working when, in reality, they aren't. It is CRITICAL to continually monitor and test data backups.

Here is another...

A Fairfax, VA, organization that became a BeckITSystems' client **AFTER** a major data loss learned their lesson the hard way, which is all too often the case. Their backup appeared to be working, but when they needed to restore financial data the most, it failed to restore. They had to recreate almost three month's worth of data because the backup was corrupted and could not restore the data. The office manager was responsible for changing tapes, but no one tested the backups to make certain data was restorable. All the computer backup logs and reports noted backup and verify completed without errors. The backup itself was faulty even though the system reported that it was working normally. **"Since starting with BeckITSystems' Continuous Data Protection Program, this is not an issue. The backup systems are monitored 24x7. Monthly test data restore jobs are performed by BeckITSystems, Inc. and status reports are provided monthly."** Kelly, CEO.

Why Trust Your Remote Backups To BeckITSystems?

There are a lot of companies offering remote backup services, so what makes us so special? Why choose us over the dozens of other companies offering what appear to be the same services? I'm glad you asked because there are 5 BIG reasons to trust us with your data security:

1. Our state-of-the-art data centers are managed to world class industry certified standards for continuity, security, and environmental specifications. This means your data is locked down tight, protected from even the worst natural disasters--fire, flood, and theft. Our data centers are located in the Western USA and Eastern USA major cities with very large communications connections that allow your data to quickly reach each center's storage facilities. This service meets all applicable standards including HIPAA and GLBA.
2. We unconditionally guarantee the security and availability of your data or your money back. If the data is given to us, we will guarantee it will be available to you 24/7 or we will give you your money back!

Most remote backup services try to promote money-back guarantees, but if you read the small print, they only refund the last 3 months of service fees. We're willing to put our money where our mouth is and give you a full year's service fees back if we fail to make your data available.

3. Support to recover lost data is **INCLUDED** with our data backup service. Some companies charge you extra for this service, or don't offer it at all. Also included with the service is a state of the art backup appliance which is a very powerful and multifunctional server. This assures you of reliable managed data backup for the affordable cost of this service.
4. We include disaster recovery services if ALL of it is lost at one time. Again, most companies charge extra for this, or they don't offer it at all. At no additional charge, we will work directly with your IT manager or network support consultant to restore data in the event of a catastrophic loss.
5. BeckITSystems is a company headquartered in Northern Virginia with real, live office, staff, and available 24x7 by toll-free phone. That might not seem too unique to you, but what you may not realize is that some offsite data companies are made up of a couple of guys working from their back

bedrooms with no way of actually reaching them other than by e-mail.

We will come on site, shake your hand, and buy you a cup of coffee. Wouldn't you rather deal with a local company that can meet with you face to face rather than an unknown entity in a different state – or different country?

6. We conduct monthly test restores of your data to confirm that your backup is working and your data is recoverable. There is no other way of knowing for sure and MOST remote backup services do NOT offer this service.

HERE IS THE BEST PART!!

While it is unlikely you will ever need to recover from a loss of data or a disaster, in the event of any interruption, BeckITSystems will restore your data AND your server functions within **HOURS** instead of days or weeks. The backup appliance that is included with our backup service has the ability to assume the functionality of the failed server to get your business up and running fast, even while a broken server is repaired or replaced.

Should you experience a loss of your servers from vandalism, flood, fire, or other problems, a replacement backup appliance will be delivered to your office by express delivery ready to work as your server or to restore data to new servers.

BeckITSystems, Inc. understands that it is essential to return to operations as fast as possible and we do it for you!

Don't Take Our Word for It – Hear What Our Clients Say

Steve, Founder and President of a specialized law firm with multiple locations wrote:

I have always found Ed and BeckITSystems to be an honest businessman with impeccable values and ethics. BeckITSystems is honest, fair, and affordable. You are constantly searching for better ways to help my offices run more efficiently and help us receive better return on our technology investment. For a small firm like mine that is mission critical. Ed, you and your creative team of professionals have made a significant contribution to the wellness and growth of my business!

Ann, Branch Chief for a National Newspaper wrote:

I can't tell you how grateful I am for your over-the-top service and thoughtfulness! Giving us Saturday service on less than one day's notice was incredibly generous and helped us out of a major jam. You and your firm are truly among the most professional, cordial, and competent I have ever dealt with!

Heidi, Director of Administration for a document management firm wrote:

BeckITSystems, Inc. always completes the work we need in a timely manner with NO SURPRISES! Their responsiveness to our needs is excellent. Their engineers and staff always go above and beyond our expectations and always with a smile.

Cindy, the owner of a disaster restoration firm wrote:

I know there are many technology companies, but I think the thing that sets BeckITSystems, Inc. above the rest is the sincere regard that all the people at BeckITSystems have for their clients. So many times I work with companies that forget that they are in business for the customer. The thing I admire most about BeckITSystems is that they always put the Customer's needs first when they do business. As a business owner, I respect the way BeckITSystems does business and I feel honored to be able to do business with such a wonderful company.

Phil, Managing Partner for a mid-sized law firm wrote:

I am the managing partner of a law firm with offices in the District of Columbia representing clients throughout North America and internationally. We have been privileged to work with BeckITSystems, Inc. on a wide range of technology issues. BeckITSystems, Inc. has proven itself to be invaluable to our efforts to utilize all available technological advancements without disruption, and without any sacrifice of quality or of our traditional commitments to clients. BeckITSystems converted our firm to a paperless office. More important, however, is the devotion of everyone at the company to the highest possible professional standards. Each BeckITSystems' professional is dedicated, farsighted, and conscious of businesses' goals and budget concerns. We are delighted to be associated with them and look forward to their assistance and friendship for years to come.

You are Under No Obligation to Do or Buy Anything When You Say “Yes” to a Free Data Security Analysis

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, I will give you my personal guarantee that you won't have to deal with a pushy, arrogant salesperson because I don't appreciate heavy sales pressure any more than you do.

However, I cannot extend this offer forever because time and staff limitations simply won't allow it. In order to secure your Free Security Analysis for your organization, please **respond to by March 31, 2012**. The numbers of free services we provide ARE limited so act today. We will make this offer available for someone else if you are unable to respond on time.

Call me immediately at (703) 433-0730 to schedule your free service, or complete and fax back the enclosed form.

Sincerely,

Ed Becker

BeckITSystems[®]
Inc.

Ed Becker, President

P.S. Don't miss out!!! Your Free Data Security Analysis (\$450 value) will let you know for sure if your backup really is copying and storing all of the data you cannot afford to lose in a format that can be restored.

Scary But True Facts About Data Loss

- The average failure rate of disk and tape drives is 100% - ALL DRIVES WILL EVENTUALLY FAIL.
- Only 34% of organizations test their tape backups and, of those who do, 77% have found failures.
- 60% of organizations that lose their data will go out of business within 6 months of the disaster.
- Over 1/2 of critical corporate data resides on unprotected PC desktops and laptops.
- Key causes for data loss are:
 - 78% Hardware or system malfunction
 - 11% Human error
 - 7% Software corruption or program malfunction
 - 2% Computer viruses
 - 1% Natural disasters
 - 1% Other
- Only 25% of users frequently back up their files, yet 85% of those same users say they are very concerned about losing important digital data.
- More than 22% said backing up their PC was on their to-do list, but they seldom do it.
- 30% of organizations report that they still do not have a disaster recovery program in place, and 2 out of 3 feel their data backup and disaster recovery plans have significant vulnerabilities.
- 1 in 25 notebooks are stolen, broken or destroyed each year.
- Today's hard drives store 500 times the data stored on the drives of a decade ago. This increased capacity amplifies the impact of data loss, making mechanical precision more critical.
- You have a 30% chance of having a corrupted file within a one-year time frame.

Source: VaultLogix

“Yes! Sign me up for a Free Data Security Analysis so I can know for sure that my data will be there when I need it!”

Please reserve one of your FREE Data Security Analyses in my name. I understand that I am under no obligation to do or to buy anything by requesting this free service.

At no charge, we will send a data security specialist to your office to:

- Audit your current data protection including backup and restore procedures, tape rotations and maintenance schedule to see if there is anything jeopardizing your data's security.
- Review procedures for storage and transportation of data. Many people don't realize they damage their disks (and thereby corrupt their data) by improperly caring for their storage devices.
- Check your network backup system to make sure it is accurately backing up all of the critical files and information you would NEVER want to lose.
- Present a simple and easy to understand chart that will detail the makeup of your data, including the age and type of files you are backing up. Why should you care? Because many organizations inadvertently use valuable computer storage to back up their employees' personal MP3 files and movies.
- Discuss current data protection 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.

BeckITSystems[®]
Inc.

Please Complete and Fax Back:

Name: _____
Title: _____
Organization: _____
Address: _____
City: _____ State: _____ Zip: _____
Phone: _____ Fax: _____
E-mail: _____

Fax This Form To: 571-287-2530
or Call: 703-433-0730