

FREE REPORT:

**“12 Little-Known Facts and
Insider Secrets *Every* Business
Owner Should Know About
Backing Up Their Data and
Choosing a Remote Backup
Service”**

**Discover What Most IT Consultants Don't
Know Or Wont Tell You About Backing Up
Your Data And Recovering It After A Disaster**

By Igor Pinchevskiy
President, IT Support LA
www.itsupportla.com
Phone: 818-797-5300

A Letter From The Author: Why Did We Create This Report And Who Should Read It



Igor Pinchevskiy
CEO
IT Support LA

From The Desk Of: Igor Pinchevskiy
CEO, IT Support LA

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 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*.

And even though many people KNOW they should be backing up their data, we have found that most business owners are grossly misinformed about data back and (more importantly) disaster recovery.

That's why we created this report. We wanted to give CEOs and executives an informative, easy to read guide that would explain what they need to know about backups, security and business continuity (a \$.50 word for keeping your business up and running).

Just by asking for this report you are putting yourself far ahead most business owners who never get around to thinking about this issue until it's too late. For that, I congratulate you and hope that you find in this report the information and the encouragement that you need to put the proper systems in place now so you can sleep easier at night knowing you're prepared for the worst.

Dedicated to serving you,

Igor Pinchevskiy

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

After working with over 300 of small and mid-size businesses in the Los Angeles area, 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, 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 tape backup. But know this:

The average failure rate for a tape backup is 100% - ALL tape backups fail at some point in time.

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

That's why history is riddled with stories of companies losing millions of dollars worth of data. In almost every case, these businesses had some type of backup system in place, but were sickened to find out it wasn't working when they needed it most.

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. 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*)

Backing Up To The “Cloud:” What It Means And Why EVERY Business Should Have It In Place

One of the BEST ways to protect your data is to maintain an up-to-date copy in a high-security data center somewhere other than your office. In fact, it should be in another “safe” city at least 180 miles away from your office, and ideally one that is not susceptible to natural disasters like hurricanes, floods, tornados or earthquakes. The generic term people use to describe this type of backup is “backing up to the cloud” or “cloud backups,” which simply means that your data is hosted in a remote data center and accessed via the Internet.

This type of backup is set to run automatically either after hours, when most people are not using their computer systems (1:00 a.m. for example), or continuously throughout the day whenever a file is changed or added. The data on a particular machine is copied and sent over the Internet to a high security facility where it is stored. Because these backups are automated, you don’t have to worry about someone forgetting to run the backup.

As with anything, you get what you pay for, and there are some key quality differences in the type of backup service you choose. Pick the wrong one and 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.

12 Critical Characteristics To Demand From Your Backup Service and IT Company

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. **Production-Grade, SAS 70 Data Center.** One of the first things you need to ask your IT person is, “Where will my data be stored?” After all, we are talking about your financial information, client data, and other sensitive information about your company! What you DON’T want is for them to keep your data at a rack in their office that is not designed to be a high-availability data center. A TRUE data center will be 100% dedicated to hosting data and should have:

- ✓ Redundant power sources and generators
- ✓ High-level, on-site building security
- ✓ Redundant Internet access
- ✓ SAS 70 certification

The term “SAS 70” (Statement on Auditing Standards No. 70) refers to an official document issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). The AICPA sets out the auditing standards for data centers and issues this document to show that the data center is doing what they are promising in the areas of security and availability.

2. **Bare metal imaging.** This is important to ensure a quick restoration of your data and IT operations. A “bare metal” image is simply a snapshot of your server and all the data on it. That snapshot can then be copied to another server or “virtualized” (put on a server online), often within 1 hour. Without this type of backup, you would have to:

- ✓ Locate all your software disks and keys
- ✓ Re-install the operating system
- ✓ Re-install all applications
- ✓ Re-install the data
- ✓ Re-configure the settings

This process could take anywhere from one to two days; even longer if you don’t actually HAVE your software discs and keys. A bare metal image eliminates this delay.

3. **The ability to recover data FAST.** An EXTREMELY important question to ask is, “If my server crashes beyond repair, how do we get our data back?” You do NOT want Internet download to be your only option for recovering data from the cloud because it could take days or weeks. At a minimum you should be able to get an overnight copy of your data on a physical disk or device – but ideally you should have instant access to a bare metal image so that a new or makeshift server can be set up within an hour, allowing you to keep working (see above).

4. **Continuous backup.** Another feature to look for is ongoing or “continuous” backup versus a nightly backup. This allows you to restore a file that you worked all morning on and saved right before the server crashed in the late afternoon.
5. **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, city-wide power outage or natural disaster destroys one of their locations, they have backups of your backup in a different city where the disaster did not strike.
6. **The INITIAL backup should be to a local, physical device.** Trying to transfer all the data online could take days (possible weeks) and cause your Internet connection and systems to drag. If you have a large amount of data to backup, ask your provider how the initial backup is created.
7. **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 damaged in a fire, stolen, or destroyed in a flood, you’re left without a backup.
8. **The ability to “virtualize” your server.** This is a fancy term for putting your server online so that you and your staff can work remotely if necessary. This option would be important if your building were destroyed or if your area were evacuated.
9. **Demand a local “spare” server and backup.** Most server crashes are due to hardware failure, not natural disasters. Therefore, you should have an onsite, local backup server as a failover device if your main server dies. This local server also makes it much easier to retrieve a file or folder than trying to pull it down from the Internet (see #3).
10. **Demand daily status reports of your backup.** All backup services should send you a daily email 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.

11. **Demand LIVE monitoring by a qualified technician.** Many online backup services are “self-serve,” which allows them to provide a cheaper service to you. BUT backups are not “set it and forget it” processes so don’t settle for an “automated” monitoring service. All too often problems happen with backups that require someone who knows what they’re doing to investigate the problem and resolve it. Otherwise, you simply have an alarm system that no one responds to. Plus, if you need to recover your data, you want to be able to call and talk to someone who can help you, especially if it’s a major disaster. If you’re using a cheap online backup service or a company that doesn’t offer live monitoring, you’ll be stuck trying to recover your data on your own, wasting tons of time and possibly not being able to get back up and running for days.
12. **Demand a written IT disaster recovery plan.** This shows YOU that they have a plan in place for restoring your data and that they won’t be scrambling to figure it out when disaster strikes. As the saying goes, “by failing to plan you’re planning to fail.” A written report shows you that they have thought the process through and know what to do in the event of a disaster

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

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 is able to 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 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 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.

Want To Know For Sure If Your Data Backup Is Truly Keeping Your Data Secure?

Our Free Data Security Analysis Will Reveal the Truth...

If you are worried about whether or not your current backup and security processes are up to par, I'd like to give you a Free Data Security Assessment (\$297 value) as a means for introducing our services to you. Why do we do this? Simply because I know how confusing and difficult it can be to find a good IT support company that is responsive, easy to work with and actually knows what they're doing.

Just about anyone can say they are an "IT expert." And since most business owners don't have the ability to evaluate whether or not their IT company or person is doing a good job, we find that offering this free service is a great, no-risk way of demonstrating how we can help you. At the very least, you'll get a free, 3rd party evaluation of your current backup, which is extremely valuable even if you don't choose to hire us.

At no charge, a security 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 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 companies 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.

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 Unified IT Service.

Naturally, I don't expect everyone to become a client; you won't be pressured into buying anything or driven nuts by pushy, desperate sales guy. Of course, we'd love to have you as a client, but our primary goals are to provide value in advance, to educate you and other business owners and to provide smart, affordable options for making sure your business doesn't lose critical data.

But I Don't Need a Free Security Analysis Because My IT 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 companies "test" their data backup and restore solution. We are helping companies like yours **AVOID** embarrassing and extremely costly data catastrophes like these:

The President of an association thought their data was being backed up safe and sound every night and he wasn't interested in looking at any other form of backup solutions. He shared with us that he had an IT guy who was responsible for maintaining the backup and had spent thousands of dollars on a highly sophisticated tape system and software. Of course, the day came when the server crashed suddenly and could not be rebooted. Fast forward three weeks, \$62,000 and a **BRAND NEW IT PERSON** later, they restored the data to as close to "before failure" as possible (much of the data was lost forever). The President of this association (who understandably asked to remain anonymous) told us the worst part of the whole experience was the frustration of spending a lot of money to avoid this type of disaster, only to discover that the systems and solution you have in place only **APPEARED** to be working, when in fact they never were.

Another client of ours learned their lesson the hard way, which is all too often the case. The tape backup appeared to be working, but when he needed it most, it failed to restore. They had to recreate almost a month's worth of data because the tape failed. In the Director of IT's own words, "I had my bags packed and was ready to be shown the door. The only reason I have my job today is because I proved to my boss that all indications were the data was being backed up. All the logs and reports noted that the backups and verifications were completed without errors. The tape just didn't work."

The Top 7 Reasons Why You'll Want To Outsource Your IT Support To Us:

1. **We Respond Within 5 Minutes Or Less.** The average amount of time it takes for one of our clients to get on the phone with a technician who can start working on resolving their problem is 3.5 minutes. We know you're busy and have made a sincere commitment to making sure your computer problems get fixed FAST. And since most repairs can be done remotely using our secure management tools, you don't have to wait around for a technician to show up.
2. **No Geek-Speak.** You deserve to get answers to your questions in PLAIN ENGLISH, not in confusing technical terms. Our technicians will also not talk down to you or make you feel stupid because you don't understand how all this "technology" works. That's our job!
3. **100% No-Small-Print Satisfaction Guarantee.** Quite simply, if you are not happy with our work, we'll do whatever it takes to make it right to YOUR standards without charging you for it. And if we can't make it right, the service is free.
4. **All Projects Are Completed On Time And On Budget.** When you hire us to complete a project for you, we won't nickel-and-dime you with unforeseen or unexpected charges or delays. We guarantee to deliver precisely what we promised to deliver, on time and on budget, with no excuses.
5. **Lower Costs, Waste And Complexity With Cloud Solutions.** By utilizing cloud computing and other advanced technologies, we can eliminate the cost, complexity and problems of managing your own in-house server while giving you more freedom, lowered costs, tighter security and instant disaster recovery.
6. **We Won't Hold You Hostage.** Many IT companies do NOT provide their clients with simple and easy-to-understand documentation that outlines key network resources, passwords, licenses, etc. By keeping that to themselves, IT companies hold their clients "hostage" to scare them away from hiring someone else. This is both unethical and unprofessional. As a client of ours, we'll provide you with full, written documentation of your network and all the resources, software licenses, passwords, hardware, etc., in simple terms so YOU can understand it. We keep our clients by delivering exceptional service — not by keeping them in the dark.
7. **Peace Of Mind.** Because we monitor all of our clients' networks 24/7/365, you never have to worry that a virus has spread, a hacker has broken in or a backup has failed to perform. We watch over your entire network, taking the management and hassle of maintaining it off your hands. This frees you to focus on your customers and running your business, not on your IT systems, security and backups.

See What Other Los Angeles Business Owners Are Saying:



"I had some Network issues and I grew tired of having my IT guy coming and check any issue after a week of annoyance, and then having him nickel and dime me for anything he does. I was referred to IT Support LA by another colleague who told me only good things about them and they had this amazing offer of 2 hours free IT consultancy which I took and what I like the most was that they were listening to my issues and suggesting solutions that I actually

understood, using a language I actually understood and not that computer jargon some people are using.

They respond to all my issues within 60 minutes and solve all my issues same day and after they do, they even explain and educate me what I did wrong or what happened so that I will be aware of that issues next time. I appreciate all the help and expertise!" - **Alex Mirzaian**, *Epic Auto Leasing*



"IT Support LA will jump through any hoops to get you what you need and the service offered by IT Support LA is unmatched by any provider I've dealt with in the past. Using IT Support LA just once will have them doing whatever they can to beat prices, offer service and value to ensure they get your return business." - **Marco Belmonte**, *Ria Financial*



"IT Support LA has helped me to lay down the IT foundations I needed for my growing business.

Now that my practice accelerates and we need to make sure everything is backed up and running well, their design at early stage really helped us transition to bigger and more complex infrastructure without us suffering from any lack of process or design flaws.

IT Support LA has been crucial to my growing business and I really don't think I would be relaxed about growing my business if I didn't have them and had to "figure out things" on the fly like others have to do. I truly cherish their expertise and everything they have done for my practice." - **Matthew Kanin**, *Law Office of Matthew Kanin*



“In our line of work, we need to have very good data security and data backup to protect our clients’ data. Now that IT Support LA has set up my backup, I have complete peace of mind that it’s all safe and secure – and it’s great not having to worry about my clients’ data. I feel that it’s much better to have a total backup solution that you just don’t need to worry about.” – **Dr. Ogden Page**, *President, Ogden Page Accountancy Corp.*



“WOW! That is all I can say about Igor and the team at IT Support LA! It’s so nice to know that our entire network is handled so I have one less crisis to deal with in my already crazy-busy schedule. I’ve worked with a number of other computer consultants in the past and no one can touch their level of service or expertise.” – **Dianne Pesgado**, *Office Manager, ABR Inc.*



“I like being able to call for IT help and get a near-immediate response. Recently I arrived at my office to find that I was unable to access documents on the network server from my workstation. I was under a court deadline and needed immediate access to the documents. I called IT SUPPORT LA for help. Within 60 minutes I had a tech working on the problem. I don’t spend valuable (billable) time solving IT problems. Also, having IT SUPPORT LA do the IT work has provided invaluable continuity of the IT solutions used in my law firm. Thanks!” – **Edward W. Pilot**, *Edward Pilot Law A Professional Corporation.*



“Before hiring IT Support LA, our network would go down regularly, run slow, and even run into the occasional virus. Since signing up for their network maintenance plan, we haven’t had one single issue. I’m VERY glad we hired these guys to support our network.” – **Ella V. Realtor**

What To Do Now

To request your Free Remote Access Consultation and FREE Home Office Action Pack,” do one of the following:

1. Fill in and fax back the enclosed request form.
2. Call me direct at 818-797-5300
3. Send an e-mail to igorp@itsupportla.com with the words, “Security Audit” in the subject line. Be sure to include your company name, address, and phone number so I can follow up with you.

David Mercy, VP of Business, from our office will call you schedule a convenient time for us to meet for 30 minutes.

Remember, there is no obligation for you to buy or do anything – this is simply a discovery meeting to see if remote access is right for you.

Dedicated to serving you,



Igor Pinchevskiy, CEO

Call me direct: 818-674-4414 or E-mail: igorp@itsupportla.com

Web: www.itsupportla.com

P.S. If you would like to speak to a few client references prior to our meeting, simply contact us and we'll be happy to provide the names and phone numbers for several clients we've worked with.

P.P.S. Please make sure you visit our web site to see the incredible 100% Money-Back Guarantee that we put on our services. You won't find another IT consultant in Los Angeles who is confident enough in their services to put as bold a guarantee in writing as the one we have.

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 companies test their tape backups and, of those who do, 77% have found failures.
- 60% of companies that lose their data will go out of business within 6 months of the disaster.
- Over ½ 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 PCs was on their to-do list, but they seldom do it.
- 30% of companies 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 most!”

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 companies 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.

Please Complete and Fax Back:

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

Fax This Form To: 1-818-804-3399

Or Call: 1-818-797-5300

A Final Word...

I hope you have found this guide helpful in shedding some light on backing up your data and making sure you could recover quickly in the event of a disaster. Clearly this is not a matter to be taken lightly, yet most business owners are so busy they don't think about it UNTIL a disaster happens.

As I stated in the opening of this report, my purpose in providing this information is to help you make an informed decision and avoid getting burned by the many incompetent firms offering these services.

Even if you feel everything is "okay" and that your current backup system is solid, I would encourage you to take me up on the offer of a Free Data Backup and Security Assessment. This assessment is, of course, provided for free with no obligations and no expectations on our part. I want to be clear that this is NOT a bait and switch offer or a trick to get you to buy something. My reputation for running an honest and trustworthy business is something I hold very dear. I would never jeopardize that in any way. So please, take a moment now to give me a call. You'll be very glad you did.

Dedicated to serving you,



Igor Pinchevskiy
CEO, IT Support LA
818-797-5300
igorp@itsupportla.com
www.itsupportla.com