LAN LOGIC

How to Avoid the Top 3 Mistakes Companies Make in Disaster Recovery

✓ **WHY DATA BACKUPS ARE INSUFFICIENT IN DISASTER RECOVERY**
✓ **HOW TO ASSESS YOUR REAL RISK TOLERANCE**
✓ **HOW TO CREATE A COMPREHENSIVE DISASTER RECOVERY PLAN**
✓ **WHY YOU NEED TO TEST YOUR BACKUPS AND PLANS BEFORE DISASTER STRIKES**

DISASTER RECOVERY IS MORE THAN A BACKUP

Backups are the first, but not the only step when protecting your data.

UNDERSTANDING YOUR RISK TOLERANCE

How long can you continue to run your business without your network or access to your data?

WRITING A DISASTER RECOVERY PLAN

How do you create a disaster recovery plan that supports your risk tolerance?

TESTING YOUR PLAN

Why test your backups and recovery plans?

WHY DATA BACKUP ISN'T ENOUGH

A lot is written about how to protect data from accidental deletion to total loss from a natural disaster. Business owners want to protect themselves and their operational data from unfortunate events, which can adversely affect their businesses. Moreover, if they are taxed by legal compliance around their business data systems, they must also consider preserving historical data as well.

While a comprehensive data backup is one of first protection measures that you can take to reduce risk, it is not until faced with a real data disaster scenario that many business owners realize the mistakes they've made in placing too much faith in the "data backup" procedure alone. Here's how making a few minor adjustments can make a world of difference in reducing the time and cost of data recovery.

GET REAL ABOUT YOUR RISK TOLERANCE

How long can your business "be down" without access to its computer network or key applications? Many business owners and leaders tend to cheat or guess when answering this question, usually in order to reduce the cost of implementing a protective measure or because they underestimate the scope of what is involved. This is a disservice to your business and makes tense times worse – especially when you told your IT service provider that you could be down for 3 days, but in reality, it's much less.

Here is a quick way to estimate this risk tolerance: Close your eyes. (Yes, it's corny. Just do it.) Now imagine that you opened the office only to find out that it has been broken into over the night and ALL OF YOUR COMPUTERS ARE GONE!!! No servers, no workstations, no switches, no firewalls, nothing.

Now ask yourself, how soon do you want to be up and running at full operation again? This is closer to your real risk tolerance. See how this "gut reaction" compares to your stated risk tolerance ? Are they close? They should be.

HAVE A COMPREHENSIVE PLAN

Simply put, "restore the backup" is not an adequate disaster recovery plan. In the previous mental exercise, you imagined the worse. Now ask yourself:

✓ How will I let employees know what happened?
✓ What will I tell customers?
✓ How are we going to take orders or set appointments?
✓ How are we going to invoice customers?
✓ How are we going to process payroll?
✓ Who all do I need to contact?
✓ How do I get started?

Now you are starting to grasp what a disaster recovery plan needs to include. And please note: None of the above questions even mentions restoring backups.

A plan does not need to be too formal, but it does require that you think about "critical business operations" and "levels of functionality." Your plan should be simple enough that any one of your managers could execute it in your absence. Include contact lists, insurance numbers, scripts for phone calls, and step-by-step procedures.

How to Avoid the Top 3 Mistakes Companies Make in Disaster Recovery

Having this plan is a HUGE step forward towards disaster preparedness! It should be in the "Top 3" priorities for your company this year, if you don't have it completed already.

TEST BACKUPS AND PLANS

Having a disaster recovery plan and data backups are GREAT steps! However, testing these on a regular basis is the only way you can rest assure that you are indeed protected. The worst time to find out that your backup jobs are corrupt or not usable is when you need them in the middle of a disaster recovery.

It may seem cost-prohibitive to test backups, but there have been great advances in both technology and pricing that can save you both time and money. The old saying, "You're only as good as your last backup," in reality is, "You're only as good as your last SUCCESSFULLY TESTED backup." Likewise, a disaster recovery plan can be "tested" in a phased manner that will allow the procedures to be verified without slowing down normal daily operations. For example: Emailing your insurance agent to verify contact information and updating claim forms and procedures is a message that can be crafted once, saved and delivered multiple times over the course of a few years.

The bottom line: Your business is the result of your hard work. Testing out the plans for dealing with adversity ensures that you can do so effectively when required and that your hard work is protected.

Be Prepared

Be prepared is more than a Boy Scout's motto. A disaster of some kind is inevitable. While it is easy to be lulled into a false sense of readiness by having regularly scheduled backups, it is more important to understand your true risk tolerance, make recovery plans that match that tolerance, and regularly test out those plans!

Lanlogic can assist you in developing your disaster readiness plan. For more information contact us today, and we can talk about your particular situation.

SERVICES AVAILABLE

- ✓ IT Services & Support
- ✓ Cloud Computing/SaaS/Hosting
- ✓ IT Consulting & Project Management
- ✓ IT Assessments & Planning

FOR COMPANIES OF ALL SIZES
On-time. On-budget. Guaranteed.

248 Rickenbacker Circle
Livermore, CA 94551
925-273-2300
888-LANLOGIC
www.lanlogic.com