Strong Technology

NEWSLETTER

Cloud Backup and Disaster Recovery - Preparing for the unexpected

- Natural Disaster - Arson - Theft - Ransomware - File Corruption - Hard Drive Failure - User Error - Power Outage - Accidental Deletion - Software Error - Virus Infection - CPU Failure -

Will you be ready when disaster strikes?

The consequences of lost data can be far reaching - leading to decreased production, revenue loss, expensive recovery costs, and in some cases, additional fines and legal repercussions.

"70% of small businesses in the U.S. experienced a data loss in the past year due to technical or human disasters"
- AMI-Partners

Disaster Recovery Planning:

Because disasters can happen at any time, knowing **how** your data is going to be recovered should be at the forefront of your organization's disaster response strategy. Strong Technology can help you plan for the worst by working with you to develop a Disaster Recovery Plan that meets your office's specific needs, testing it to ensure that you will have access to the information you need, and implementing it in case of emergency.

5 Key Elements of Recovery:

1. Speed- Define a recovery time objective (RTO)
2. Scope- Address the unique needs of each part of your business
3. Timespan- Set a plan for Short, Medium, and Longterm goals
4. Granularity- Think about recovery on multiple levels
5. Testing- Test the plan regularly and make improvements

Unfortunately, simply "having" a backup isn't enough to protect your business from a data loss disaster. Backups only work if they include the right data, and are performed regularly and correctly.

Intronis Cloud Backup + Recovery:

Having a current and complete backup is critical to your recovery process. Here's why we use *Intronis Cloud Backup + Recovery*:

- Helps minimize the risk of data loss
- Scalable, and can't be lost, stolen, or damaged
- Data can be restored anytime, anywhere
- Military-grade data encryption maximizes security
- Allows us to remotely test and monitor your daily-backups to ensure that they have been successfully uploaded

Key Steps in Creating a Disaster Recovery Plan:

1. Establish a planning group including key people from each business unit
2. Perform Risk Assessment and Audits - Assess impact to each role in organization
3. Establish priorities for applications (Mission Critical, Critical, Essential, etc)
4. Develop recovery strategies
5. Prepare inventory and documentation of the plan
6. Test the plan ...And, if disaster strikes...
7. Implement the plan

What Data Should I Backup?

- Business Applications
- Customer Data
- Financial Data
- Software Programs
- Email Systems
- Payroll Info
- HR docs / Employee Info
- And more

LEARN MORE:

Additional knowledgebase articles and training resources can be found online at www.strongtc.com/resources.html

Stay up to date on all of the latest IT security news by following Strong Technology on: