Azure Disaster Recovery and Backup Blog Post #2

|  |  |
| --- | --- |
| Keywords | Business continuity  Disaster recovery  Site recovery  Microsoft Azure  Azure backup |
| Target Audience | Small to mid-sized business owners (low tech)  mid-sized business IT managers (technical, but short on resources) |
| Headline #1 | 5 steps to a solid disaster recovery plan. |
| Headline #2 | No backup plan? It could cost you thousands of dollars. |
| Headline # 3 | Your idea (edit your post after a week and change the headline to see which headline gets the most views). |
| Call to action #1 | Join us on [date] for a free webinar about Disaster Recovery and Backup for your business. |
| Call to action #2 | Download our e-guide for more information about a disaster recovery plan. |
| Call to action #3 | Your idea |

**Body copy**

If your business was about to be destroyed by fire, and you had one minute to save one file, what would it be?

I’d guess not your pictures of Fluffy the cat. But maybe your payroll data or customer order list. A Disaster Recovery strategy defines which data you will save first and what will be available during planned or unplanned downtimes. It also plans for the data you can live without. Poor Fluffy.

**Complexity vs. Costs**

When you create your Disaster Recovery plan, you’ll need to weigh the trade-offs between complexity vs. costs. What data can you afford to be without? For how long? If you lost some data, would that destroy your business forever?

**Five parts of a disaster recovery plan:**

1. **Recovery Point Objective (RPO).** RPO defines how much data you are willing to lose. You can give higher priority to your most critical data, but be willing to lose less important data, such as pictures of Fluffy. Customer records might be top of your list, while marketing data might rank lower.
2. **Recovery Time Objection (RTO).** RTO weighs how long you are willing to be without your data. Depending on your business, you might decide that you can lose up to two hours of business operation. A shorter time will create higher costs, so you’ll need to consider your options carefully.
3. **Personnel.** Who should get their data back sooner? Who will support the plan? Do you have a backup person as well as backup technology? Is your plan dependent on human intervention, which may not be possible in all cases?
4. **Regulatory constraints.** Is your business subject to regulatory compliance? How will you make sure you are covered?
5. **Critical data.** Which data is critical to your business? What are the dependencies between different areas of the business?

**Test and train**

Often companies will create a plan, and then leave it on the shelf. They don’t fully test the plan, or consider multiple scenarios. When a disaster hits, whether it’s cybercrime or a hurricane or a rogue sprinkler system, the plan fails. The New York Stock Exchange had a plan before Hurricane Sandy, but they didn’t follow it when disaster hit. Instead, they closed the stock exchange for two days.

Your resources and business needs will change over time. This includes your location, personnel, and data. Testing your plan two to three times a year is one way to make sure the plan is up-to-date and still supports your current business goals.

Once you have a plan in place you’ll need to train all personnel. For a higher chance of success, ensure that senior management endorses the plan and promotes training for all employees.

**Get help to create a plan**

A cloud solution can help you find a good balance between cost and complexity. With Azure Site Recovery, you can easily create disaster recovery plans in the Microsoft Azure portal. The disaster recovery plans can be as simple or as advanced as your business requirements demand.

We’re here to help you with all stages of strategy, planning and implementation.

**[Add your call to action here]**