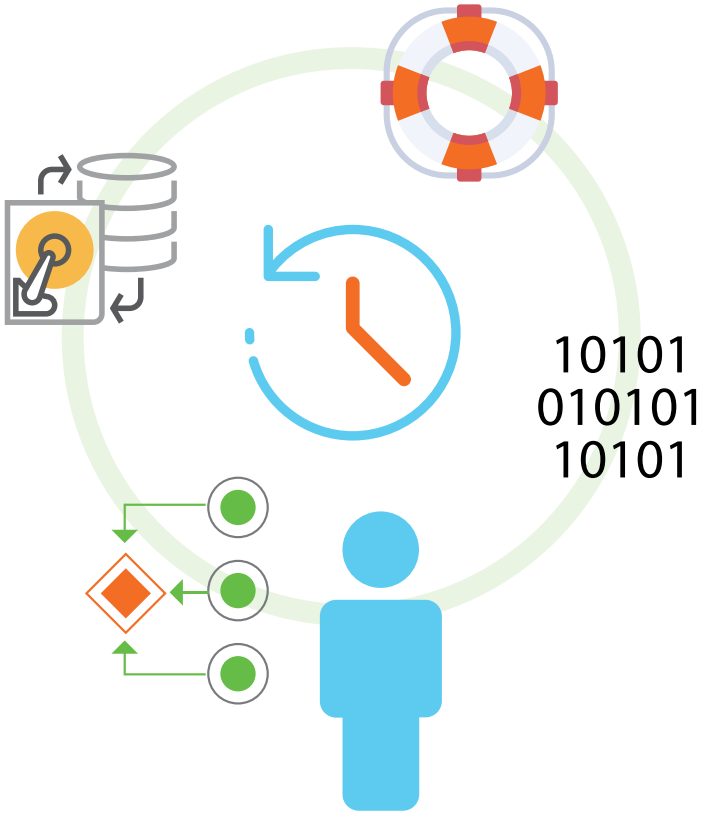
Intronis
MSP Solutions by Barracuda

Recipes FOR Success



How to Develop a Better Disaster Recovery Plan for Your SMB Customers

Disasters can strike at any time, so as an MSP it is essential for you to have a concrete **disaster recovery plan** in place for each of your clients so they'll be prepared when the worst happens. **Follow this recipe** to ensure your customers aren't missing any critical ingredients in their disaster recovery plans.

Key Ingredients:

- **Critical business processes and applications**
- **Defined Recovery Point Objectives (RPOs)**
- **Defined Recovery Time Objective (RTOs)**
- **A list of potential disaster scenarios**
- **Documented policies and procedures**
- **Time to test the plan**

Recipes FOR Success

DIRECTIONS

Intronis MSP Solutions by Barracuda

1. Evaluate your customer's business.

Start by measuring the **processes and applications** that are vital to your customer's success. Talk to multiple people at the company to get a high-level view of everything the customer would need to keep the doors open, not just the business-critical files they'd need to recover. Ask them to prioritize their top applications to get a better understanding of what needs to be restored first.

2. Conduct a risk assessment.

Next, you need to understand the rate of data churn for each application. Mix together the customer's **minimum Recovery Point Objective** (RPO) and **maximum Recovery Time Objective** (RTO) to determine how much data they can afford to lose. To avoid costly downtime, implement tighter RPOs and quicker RTOs. Determine what appropriate and realistic RPOs and RTOs would be—and make sure that you can meet them — so the customer won't be left in a scramble without their data.

3. Cook up a complete plan.

Your customer needs to be prepared to recover from a variety of disasters—from something large like a fire or flood to something small like a failed hard drive. Prepare **a list of potential disaster scenarios** and bake appropriate responses into the disaster recovery plan. Document **written policies and procedures** that your MSP will follow in each situation, along with what the customer will need to do and who will be responsible for each step.

4. Test the plan.

After you develop the plan, you need to test it. Set aside **time** to do a dry run and make sure everything goes smoothly. This step will help you uncover any flaws in the plan and gives you an opportunity to revise it before something goes wrong. A disaster recovery plan isn't just a one and done, so test your customer's plan on an annual or more frequent basis. Stir in more protection or different RPOs/RTOs as needed to fit changing requirements, and continue to test the plan on a regular basis.

Read our latest case study with Electronic & Computer Specialties to learn more about disaster recovery done right.

TIPS & TRICKS

Take a three-layered approach.

To have a successful disaster recovery plan, you need a variety of ways to retrieve the customer's data in different scenarios. Implementing a 3-2-1 data protection strategy can help. Start off by whipping up three copies of customer's data. Preserve two sets of data on different types of media, while the third data set is stored in the cloud.

Pre-heat your chances of success

Don't freeze your chance of recovering customer data after a natural disaster like a blizzard or hurricane occurs. Review the disaster recovery plan with your customer beforehand, highlight any areas the customer might be responsible for, and then check to see when the customer's most recent backup took place. Sprinkle in an extra backup before the storm hits, and reschedule backups that might be scheduled to happen during the storm to an earlier time.