LANSPEED
Your Strategic I.T. Partner

The Ultimate Earthquake Recovery Checklist

STAY ONE STEP AHEAD OF EARTHQUAKES

For businesses based on the west coast, earthquakes are an all too familiar natural disaster. Unlike hurricanes or other storms, an earthquake can hit without warning. When it comes to protecting critical business data, companies need to ensure they're prepared for an earthquake literally shaking up their data. It's not only important to have a disaster recovery solution you trust, but to make sure you test it well.

Keep this earthquake DR checklist on hand.

Prior to an earthquake ever occurring (and unfortunately it's a matter of when and not if) ask yourself the following:

- Do you have a disaster recovery solution in place?
- Do you trust it?
- When was the last time your backup was tested?
- How long does it take to recover from your current backup solution?
- How long can you realistically be down? 1 hour? 1 day?
- What is the financial cost of downtime to your business?
- When a disaster occurs, is there an offsite copy?

The earthquake has occurred—time to walk through the following steps:

□ **1. Assess the damage and its impact on your business**

Every disaster is different. Before doing anything, understand the underlying issue and how it may affect you.

- Is the issue local to one machine, or does it affect your entire system?
- Have files been deleted or are servers/workstations down?

□ **2. Establish recovery goals**

Recovery is what makes a BDR solution different from a simple backup product. Plan out your road to recovery.

- Restore the system, the data, or both? Should time be spent recovering files and folders before system recovery?
- Identify critical systems and prioritize recovery tasks.
- What date/time should you recover from?

□ 3. Select the appropriate recovery type(s)

To get to your “road to recovery”, the appropriate recovery procedure must be followed. Think about which approach will best get you to your end goal.

- File restore. *OR*
- Local virtualization. *OR*
- Off-site virtualization.

□ 4. Verify the recovery and confirm functionality with users

Once a recovery is verified, confirm that it interacts positively with users.

- Test network connectivity.
- Ensure all users can access resources and applications in the virtual environment.

□ 5. Restore the original system(s), if needed

If the original system(s) needs to be restored, decide which restoration process will work best.

- Bare metal restore. *OR*
- Virtual machine restore.

□ 6. Self-assess afterwards

After it’s all said and done, take a step back and think about it: How well did your team do? What could you have done differently?

- What precipitated the failure?
- What ongoing issues need to addressed?
- What can be done better in future DR scenarios?

Don’t have a Disaster Recovery Plan in place yet?
Not sure how to get started?

Download our free guide to writing your first complete Disaster Recovery Plan.

Download Now!