FORTIS

9-Point Disaster Recovery Checklist

What Does Disaster Recovery Mean For Your Company?

Unfortunately these days, it's not a matter of "if" but "when" a real world threat may compromise your business data. Between viruses, user error and ransomware, these threats are becoming ever-present. Imagine that your server fails. Imagine you or an employee accidentally deletes important files or a virus corrupts your systems. Imagine all your customer data disappearing.

Prepare Before a Disaster Strikes

When it comes to data backup and disaster recovery (BDR), being prepared for potential disasters is key to keep your business running. Ask yourself these questions -

- Do you have a disaster recovery solution in place?
- 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 of your data?

A 9-Point Checklist

Stay One Step Ahead Of Potential Disasters

1 Develop a Written Plan

Create a formal disaster recovery plan in case servers, local backup systems or your office are damaged or destroyed.

- Put that plan in a secured file sharing location online so it's always available.
- Be sure to keep it updated as infrastructure throughout the organization evolves.

2 Secure Your Data

The physical security of your data is critical.
Locate your server in an access controlled room to minimize accidents and/or intentional damage.

3 Consider Emergency Power

Install an uninterrupted power supply (UPS) system on mission critical servers and systems to allow for a smooth transition from primary (utility) power to emergency during an outage.

9-Point Disaster Recovery Checklist

You must also prepare for natural disasters which may render offices and computer systems inaccessible or unusable. Flooding, fire and earthquake all present very real threats to continued business operations.

4 Redundant Internet is a Must

In today's world, internet down means business down. Secondary internet connections are relatively inexpensive.

- Get a backup internet connection.
- Setup automatic failover so if the primary connection goes down, the backup will switch over.

5 Schedule Regular Local Backups

Having a local backup copy is often the fastest path to recovery. If the primary business location maintains power, backup files or entire drives can be reloaded quickly.

- Ensure you are in fact backing up all your critical data (not just servers).
- Schedule regular backups.

6 Backup Critical Data to the Cloud

Local backups are great but what if your office or server is damaged, destroyed or inaccessible?

- Use cloud-based backup service to ensure your data is available anytime, anywhere you need it.

7 Verify Your Backups

Days of down-time from missing file backups, backup failures and inability to restore data are the worst nightmare.

- Use a backup service that automatically verifies each back is free of corruption.
- Perform periodic test restores.

8 Business Continuity - telephones

Continued communication with customers and suppliers will be essential.

- Implement a VoIP telephone system which runs across the internet not telephone poles.
- Have a stash of VoIP-enabled telephones to give to employees so they can plug in at home and make/receive calls as if they were at their desk.

9 Business Continuity - systems

Key business services require uninterrupted access to business applications and information sharing.

- Utilize cloud-based applications and file storage such as Quickbooks Online, Google G Suite and Office 365 which can run from anywhere without a VPN.
- Use VoIP phones so employees can make/receive calls from anywhere as if they were at their desk.

FORTIS

www.FortisTelecom.net (916) 235-4200