

Disaster Recovery

Planning

Step 1

Identify Critical Equipment

- Servers and PCs
- The number of PCs that are required to conduct daily tasks
- The minimum number of telephones & faxes required to conduct business
- Critical staff

In addition to critical servers you must include critical PCs that control alarms, heating & ventilation systems, accounting functions, time clocks, manufacturing equipment, etc.

Identify employees, required to maintain your business. In some instances, it is your employees who may be affected and not your physical location or equipment ie. a pandemic. Employees who cannot come to work may still, with the appropriate tools, be able to work remotely.

Step 2

Ask Yourself

- Does your plan address recovery on-site at your office, or can you restore at an off-site location if such is deemed as a requirement?
- During a disaster, will you have all the same server, PC, and tape backup equipment available or have you planned for being able to restore using dissimilar hardware?
 - On the same server(s) and/or PC(s) at the same location
 - On different server(s) and/or PC(s) at the same location
 - On different server(s) and/or PC(s) at a remote location

If a critical system experiences a hardware failure, that can just be replaced under warranty. If your place of business has been destroyed or is inaccessible how long will it take you to purchase new equipment?

Tenecom provides standby PCs, Virtual Servers, and Internet access hardware that can be loaded with your critical system images if an offsite recovery is required.

Step 3

Availability

- Formalize your expectations for IT infrastructure availability
- For your critical servers & PCs, determine the maximum time at which an outage would have major economic impact on your business

The customer must know the time required to restore critical systems. There are always delays when restoring servers and PCs that involve complex configurations and large amounts of data.

Your plan should address the conditions that dictate a disaster. Server corruption, hardware failures, or adverse affects (water, smoke, theft, etc) to the environment may only last for a limited amount of time. Picking up your data and employees and rushing into disaster mode may not warrant the effort and costs.

Implementation

Backup to Tape

Pros

- Reliable if configured properly with proper hardware and software
- Media is relatively inexpensive
- Typical capacity from 100 to 800 gigabytes
- Ability to accumulate tapes and retain tapes with historical data
- Easy to remove tapes to an off-site location

Cons

- Typically not configured to backup PCs
- Backup time can be long, depending on the amount of data and the number of servers
- Restore process for a total server attached to the tape drive is slow
- Restore process for a total server, not attached to the tape drive is even slower
- If the tape drive is not available, nothing can be done
- Backup occurs at night, so anything lost during the day cannot be recovered

Backup to a NAS device (Network hard drive)

Pros

- Backup can be scheduled to run at various intervals during the day so that files lost during the day can be recovered
- Backup and restore is faster than tape
- Reliable if configured properly with proper hardware and software
- Typical capacity from 100 Gig to 2 Terabytes
- With the right software and budget, you can easily backup and restore critical PCs
- Easy to transport and use during a restore

Cons

- Devices are relatively expensive
- It is difficult to retain spare devices with historical data
- A failure or loss of the NAS device implies no backup exists

Hardware & Software Requirements

Tenecom Solutions provides a wealth of expertise in the area of Disaster Recovery for small & medium size businesses. We deploy core products from leading software and hardware vendors to address all aspects of Disaster Recovery. Call us to review your requirements and provide you with the most reliable solutions to address your Disaster Recovery concerns.