6 STEPS TO DISASTER RECOVERY PREPAREDNESS

> **"THE WILL TO WIN MEANS NOTHING WITHOUT THE WILL TO PREPARE."**
>
> *–Juma Ikangaa*

ARE YOU READY?

Companies need to protect their data, files, folders, and email, but they also must protect applications, networks, document repositories, and the ability to deliver business services within an acceptable time frame. In the event of a disaster, could you list everything your IT staff needed to recover off the top of your head? Could you give direction on which data takes priority over others, or how fast your systems need to be up and running again?

A detailed Disaster Recovery (DR) plan with clear objectives can answer these questions and help you protect data and critical IT systems, while mitigating the risk of a disaster or IT failure. But you have to be proactive in developing and testing a comprehensive DR plan to protect your business before disaster strikes.

DON'T WRITE A DR PLAN AND FILE IT AWAY

Writing a DR plan that you never test or revise is nearly as bad as not having one at all. Writing the plan is only one step of the process. You must test the plan, evaluate the results and adjust the plan accordingly.

- Production environments change constantly, so ensuring plans are routinely tested and revised as necessary is key.
- Systems that are considered mission-critical may change over time; a DR plan needs to reflect this.
- Documentation may not be complete; businesses often find that there are steps missing as the procedure is actually reviewed step-by-step.
- Testing the plan to ensure it works is an important facet of being prepared. Your DR plan may "work" on paper, but in reality may not achieve the recovery time objectives (RTOs) and recovery point objectives (RPOs) your business requires.

STEPS TO IMPROVE YOUR DR PREPAREDNESS

1 START SMALL.

Your first step is to take an inventory of all systems and applications. Work with different departments to define and identify the priorities of your business.

2 DETERMINE YOUR RPOs and RTOs.

Proper Disaster Recovery planning requires the determination of the RTO (recovery time objective) to define the maximum amount of time your business can be without IT systems post-disaster, as well as the RPO (recovery point objective) which defines the amount of data loss your business is willing to risk in the event of a disaster. Defining these metrics is critical to setting expectations for management, employees and customers.

3 DOCUMENT THE PLAN.

Fully document your disaster recovery plan by clearly identifying the critical applications and their vital components. Document the failover/failback process in detail as well.

4 TEST THE PLAN.

Make sure the recovery times and recovery points achieved during the test meet your objectives. Testing your DR process will prove the viability of your plan and highlight any inefficiencies.

5 REVISE AS NECESSARY.

Evaluate the test results and, if things didn't go according to plan, make revisions that will better prepare your business for a future disaster.

6 RE-TEST THE PLAN.

Then re-evaluate and revise. Set up a regular test schedule so that you're testing according to what makes sense for your business.

MORE TIPS

✓ **POWER REDUNDANCY IS PARAMOUNT:**
Any business running an internal data center must also pay for and attend to its power supply, which is subject to potential failures as a result of storms, car accidents, utility companies or service equipment failure. Remember: Each additional layer of power protection has an exponential increase in cost.

✓ **LOSS OF CONNECTIVITY LEADS TO MORE DOWNTIME:**
Companies that manage network connectivity in-house to support mission-critical applications are more susceptible to downtime due to a loss of connectivity, as it is cost prohibitive to design the same level of redundancy that a commercial data center provider would implement. Typically, the capital cost and monthly operating costs of establishing a fully redundant and resilient network are prohibitive for most companies, in addition to the costs of supporting such a network. As such, these companies will make use of one Internet carrier, creating a single point of failure.

✓ **LACK OF KNOWLEDGE CAN EQUAL DISASTER:**
To the best of your capabilities, you must ensure that your IT staff has a complete depth of knowledge in each technology skillset required to properly mitigate the risk of outages. If you're seeing the workload for your IT staff increasing, know that this can have an adverse effect on the availability of your systems.