DO YOU TRUST YOUR DISASTER RECOVERY PLAN?

www.TechRageIT.com

DO YOU TRUST YOUR DISASTER RECOVERY PLAN?

When is the best time for you and your team to prepare for a disaster? *Hint: it’s not during the hurricane or a cyber attack!* All businesses, with their narrow margins for error, are particularly vulnerable to the kinds of natural and human-caused disasters that can send a business into a deep freeze.

However, why is it that 68% of small and medium-sized businesses still don’t have a written disaster recovery plan[1]? Or, better yet, why hasn’t 23% of companies tested their disaster recovery plan[2], despite major risks?

Every organization needs a comprehensive disaster recovery plan. Not only does it protect vital information, it gets businesses up and running when disasters, like hurricanes, strike.

Source: 1 - Nationwide 2 - Spiceworks

But don’t be fooled into thinking only about natural disasters, disasters can also be caused by security breaches like ransomware, a hardware or software crash, or by simple human error.

If you stop to consider the recent statistics, it becomes clear that you cannot afford to be complacent when it comes to disaster recovery.

140,000

hard drives fail in the US each week.

Source: Seagate

22% of small businesses cease business after a ransomware attack.

Source: CNN

96%

of businesses with a backup and disaster recovery plan fully recover operations.

Source: Comparitech

$5,600

is the average cost of downtime per minute.

Source: Gartner

WHAT’S INCLUDED IN A DISASTER RECOVERY PLAN?

A plan includes many areas of an organization — computers, network, phones, employees and customers. What’s important is how quickly the organization can gain access to critical systems and data.

The major elements of any good disaster recovery plan includes:

1. **Data replication** – it’s crucial that all business data is regularly backed up to a separate location or to the cloud.

2 **Priorities** – decide which applications your business can't survive without for any but the shortest length of time. Which ones do you need access to within a day or so? And, conversely, which can wait a few days before it becomes a serious problem.

3 **Roles** – spell out in writing who is responsible for which aspects of a recovery, including your own employees and vendors, along with their contact information.

4 **Assets** – you'll need a thorough, current list of all hardware and major software applications, plus contact information for technical and customer service support for each item. It's important to also have a plan for protecting hardware and documents against elements such as leaks or flooding.

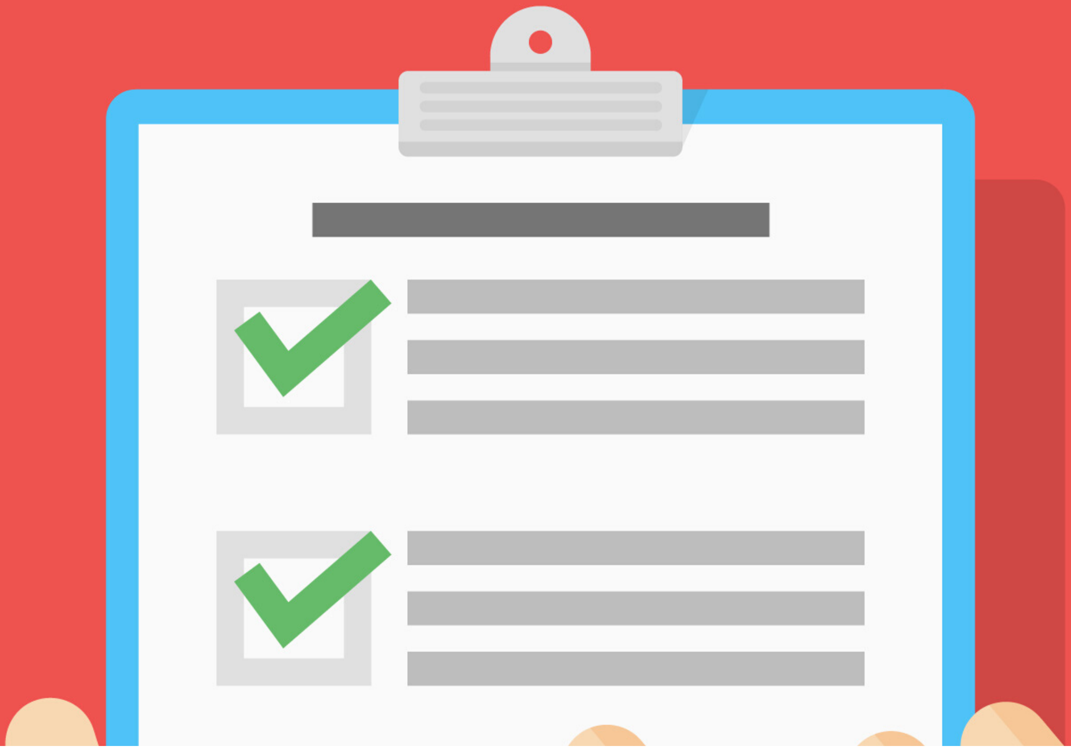
5 **Remote Working** – know how you will communicate with employees about what they should do in case of an emergency. Determine if you need digital work space technologies that allow employees to work at home or elsewhere should the office become flooded or major highways become impassable.

TEST YOUR DISASTER RECOVERY PLAN

So, you have a disaster recovery plan. The question is, do you trust it? Can your plan really recover what it needs, when it needs, in order to protect your data, applications, and security?

There's only one way to know for sure...test. Test. TEST!

CHECK LIST



Even the best disaster plans can go awry, especially if no one bothers to test them. Every disaster recovery plan needs to be tested regularly, whether it's run in-house or by a managed services provider. It's recommended to test your plan at least twice a year or when significant infrastructure changes take place.

These tests not only provide the comfort and knowledge that your disaster recovery plan works, but they can also help identify issues that may arise in an actual disaster. They train employees to know exactly what to do, and they give your staff the experience with their roles and responsibilities in an emergency situation.

When it comes to disaster recover planning, be sure you don’t neglect to do it.