StorageCraft

Make a Disaster Recovery Plan:

Your 2021 New Year's Resolution

As 2020 comes to a close, small businesses reflect on the trying year that most have faced. More than ever, this year, having a robust disaster recovery and business continuity strategy has been top of mind. Heading into 2021, all companies should be re-evaluating those plans and determining how they need to be revised. Some will have to create a plan from scratch, but it will be well worth it.

This past year brought not only a global pandemic, but it also saw a relentless series of natural disasters – all of which took a toll on small businesses:

- Most significantly, the COVID-19 pandemic has impacted almost everyone around the globe. As well as the human tragedy, the economic impact is still unfolding.
- As of October 2020, a total of 8,200 fires have burned 4 million acres in California, more than 4% of the state's roughly 100 million acres of land, which makes 2020 the largest wildfire season ever recorded in California.
- There were a record of 10 named hurricanes in September, and five storms churned in the Atlantic Ocean simultaneously.

If that weren't hardship enough, the sad truth is that while businesses struggle to survive, there is a dark force at work looking to reap even more harm. These are the bad actors using these incidents to try and create cyber vulnerability in the form of phishing and ransomware attacks. After all, it's human nature to click on a link to a charity supporting people impacted by natural disasters; or a link that seems official to local government support. Yet, all too often, they are malicious attempts to gain entry to your data.

So, as we leave the trials of 2020 and remember it as a year like no other, there is no better time to create a strategic and effective disaster recovery plan.

According to FEMA, roughly 40 to 60% of small businesses never reopen following a disaster. Also, following a disaster, 90% of smaller companies fail within a year unless they can resume operations within five days. This proves the power of a robust disaster recovery strategy.

Several factors play a role in whether a business can get up and running again. This includes strategic planning before a crisis to recover mission-critical data, applications, and systems quickly and effectively.

The following are tips to help small businesses develop disaster recovery plans and drills and business continuity plans.

What Is a Disaster Recovery Plan?

A DR plan outlines the processes and procedures to recover critical IT business data, with the prime objective of minimizing downtime after an emergency or crisis so that your business can be up and running as soon as possible.

A small business should work with its IT or managed service provider team to create a DR plan to list the steps necessary to recover networks, servers, laptops/desktops, data, and connectivity.

- **Data Protection:** A small business should ensure offsite backups are successfully running, including monitoring services and the ability to boot up a VM from the cloud as quickly as possible. As such, the DR plan should identify high-priority-servers that are hosting valuable data -- and are the most critical for prioritizing backups.
- **Cloud Backup and Recovery:** Data loss can have a long-lasting negative impact on your business. However, cloud backup offers a cost-effective and efficient way to ensure operations continue to run smoothly. Once you have your data backed up in the cloud, don't forget to determine how you recover that data and connect it back into your network. The backup and recovery go hand in hand, and you must have both pieces to complete the puzzle.
- **Colocation of Servers:** One way to guarantee that on-site servers have a backup is to consider colocation (or colors). This enables a business to rent space for servers and other hardware at a different location. This case scenario is most helpful for companies whose data or application is tightly integrated with the hardware. A DR plan should note the location and contacts for the colo provider and have arrangements to access data in times of emergency or crisis.
- **Robust VPN Solution:** Many natural disasters make it impossible for employees to reach their offices. But in many cases, employees can keep working with a reliable VPN connection from home, and therefore having a robust VPN solution is among the most important services a small business can have. A DR plan can outline who has access to the VPN and how to access VPN during crisis times.
- **Beware of Ransomware Attacks:** Remember to include a recovery strategy in your DR plan that addresses cyber-attacks. As small businesses can be vulnerable to ransomware threats, it is crucial to prepare in advance by strengthening security infrastructures, training employees to spot suspicious activity, and regularly reviewing backup and recovery strategies.

Disaster Recovery Drills:

While many small businesses conduct fire drills, they don't often consider conducting a DR drill. Yet, a DR drill is paramount to check the efficacy of disaster and business recovery plans. Four key steps to consider including in a drill are:

- **Review Your Data Disaster Recovery/Business Continuity Plans:** An excellent first step is to conduct what Georgetown University calls a "table-top exercise" with key stakeholders, including the IT department/solution provider, department managers, communication team, and vendors reviewing the plans and going over processes and procedures.
- **Test Your IT Systems/Infrastructures:** Conduct a dummy run checking the performance of critical elements of the DR plans, including backup systems, servers, applications, and more. Ensure that all business data is backed up at regular intervals so that important information is accessible after a crisis. Create lists of equipment/applications and other critical systems that fail to work during the drill.
- **Upgrade/Fix Equipment/Applications and More:** During the drill, you may notice that some systems are not operating at full capacity and might have some discrepancies. It will also be essential to discover more effective means for accessing critical systems during an emergency. This is an opportunity to work with your IT team/solution provider to fix, upgrade, and modernize your existing IT infrastructure.

Some extra resources to help create a DR plan:

- **IT Disaster Recovery Plan –** from the Department of Homeland Security
- **IT Disaster Recovery Plan Template –** from Search Disaster Recovery

How is a Business Continuity Plan Different from a Disaster Recovery Plan?

A business continuity (BC) plan can be a part of a small business' disaster recovery planning. It is additive to a DR plan, though, because it plans to recover the organization's entire operations – not just its IT systems.

A solid BC plan will include a set of risk management principals – which means, roughly, identifying all the threats to an organization's capital and earnings and outlines steps to mitigate such risks.

It will include, for example:

- Emergency team names and contact details
- Lists of mission-critical equipment
- Lists of vendors and suppliers
- Lists of vital records and critical business documents
- Lists of minimal operational requirements to resume business
- Communication plans to important company stakeholders including employees, the board of directors, customers, and more

The following is a helpful resource for Business Continuity Planning from ReadyGov.

You never know when disaster will strike or in what form. What you can do is anticipate your most significant risks and prepare for the worst. Disaster preparedness is the key to disaster recovery. Being well prepared can make a big difference in a small businesses' success and resiliency as we head into 2021.

StorageCraft