# TOP SIX DISASTER RECOVERY PLANNING MISTAKES BUSINESSES MAKE

magna5

www.magna5global.com 844.624.6255

**Developing a disaster recovery plan is essential to protecting your business from the unexpected. But many businesses fail to account for critical areas during their planning. In this white paper, we review six disaster recovery planning mistakes you cannot afford to overlook.**

The stakes of protecting business-critical data have never been higher. An unexpected ransomware attack, fire, flood or other natural disasters can easily bring an organization to a standstill. The impact of disruptive downtime can be felt immediately too, causing significant loss of revenue and customer trust.

Today's integrated networks with smart and connected devices have made data backup and disaster recovery paramount to the success of the entire lifecycle of an organization. Yet too often organizations take the reactive path of "waiting" for a cyberattack or natural disaster to occur, and then discover too late they can only partially recover their data.

Disaster recovery planning has never been more important. For unprepared businesses, the risks are severe and costly. 90% of businesses that experience a disaster and do not resume operations in five days fail within the first year. The unprepared enterprises that do survive face millions of dollars in damages.

With the rising frequency of cyberattacks and natural disasters, the future of protecting your business hinges on developing a disaster recovery plan. Unfortunately, many businesses continue to make mistakes that leave them vulnerable to disaster. Here are six mistakes to avoid while developing your disaster recovery plan.

## #1 Not Backing Up Your Data (Correctly)

Data backups are the backbone of any effective disaster recovery plan. Without a comprehensive data backup solution in place, you stand to lose financial documentation, client information and other mission-critical data.

Losing organizational data in a disaster can cost a business hundreds of thousands to millions of dollars. The good news is that this is easily preventable.

There are a lot of considerations that goes into a data backup solution (deployment models, physical vs. cloud, recovery prioritization, backup frequency). But most organizations can deploy a cloud-based backup plan that stores all their data offsite while being easily accessible for recovery should a disaster occur.

Here are a few considerations for your backups:

- **Backups should be disconnected offsite from the network:** Many organizations make the mistake of having their primary and replicated data in two data centers but shared on the same network. So, if a primary site is breached with ransomware, the second site on the shared network will also be breached. It is important to replicate data backups offsite disconnected from the network. This way, if the local backup is compromised, the secondary backup is safe and can quickly be recovered.

- **Backup storage should have strong permissions:** It is important to lock down which users and service accounts have access to the backup storage. Ideally, the storage is locked down to a single account that is not used for accessing any other systems where the credentials could get compromised.

- **All backup data should be encrypted:** Organizations handling their own cloud or on-premises data backup normally encrypt their cloud infrastructure data but not their data backup. Encrypting data before it leaves a machine, in transit and at rest on disk can ensure data is not easily decrypted.

## #2 Not Preparing for Multiple Types of Disasters

Disasters come in many forms – power outages, natural disasters, data breaches, equipment failures and even human error – and can cause serious damage if you are not prepared. While there is some overlap, preparing for one type of disaster can still leave you vulnerable to the ones you did not consider.

Responding to ransomware attacks require a much different approach than addressing water damage to IT infrastructure. An effective disaster recovery plan will prepare for multiple different contingencies and necessary responses. For example, a ransomware attack and flood will both require recovering data off a cloud backup, while a severe power outage will involve restoring access to key communication platforms. Preparing for more than just one type of disaster better protects your business from the unexpected.

## #3 Not Communicating the Plan to Personnel

As important as a recovery plan is, it is not going to do any good if no one at the company knows what it is or how it works. A plan is not implemented until you communicate it and get buy-in from employees at every level of the company. Personnel outside of IT will play vital roles in addressing the disaster. Some of these include:

- Engaging in public relations
- Assessing financial damages
- Communicating with clients and customers

Compared to other aspects of disaster planning, an easy (and free) way to bolster your defense is to effectively educate and communicate to employees on how to respond to different types of disasters.

## #4 Not Testing and Updating the Plan

Just as a plan is not useful if no one knows how to use it, a plan is not effective if you do not know that it works. That means testing the plan after you create it to see if there is a need for additional measures. This is also helpful for checking if the recovery timeline you set is realistic. It is easy to underestimate how long it will take to reinstall hardware or download a terabyte of backup data from the cloud.

Similarly, if you do not update the recovery plan, it will not be useful for long.

Remember that new enterprise software you just purchased? Add it to the plan. Personnel changes? Reassign responsibilities. Added a new location? It will need to be integrated into the plan. The only way to know you are ready for a disaster is having a realistic and up-to-date plan that has been thoroughly tested.

## #5 Not Preparing Remote Access

During a disaster, employees will lose access to hardware, communication channels and applications they need to do their jobs. Businesses that fail to prepare for this will see their productivity grind to a halt.

If the office is shut down or hardware is compromised, employees will need a computer to work remotely. Common options include remote access on personal computers and company laptops. This is made easier if endpoint data is included into your data backup strategy.

Enterprises everywhere rely on applications to get business done. Fortunately, the widespread adoption of SaaS and cloud-based software has made it easier to access applications during a disaster. In a crisis, communication channels are more critical than ever, but they are also vulnerable to long periods of downtime. Having a cloud-based communication solution in place will give you flexibility and increased uptime, both during and outside of a disaster.

It is worth investigating if you have any limitations to your software stack. License-based applications will require additional licenses for employees working on alternate computers. Software that is installed on the computer and unavailable off the cloud might require workarounds.

## #6 Not Learning from Experience

Businesses that fail to learn from a disaster will be doomed to repeat the same mistakes the next time another one strikes.

When the dust settles from a disaster, take a moment to reflect on the experience and evaluate the effectiveness of your recovery plan. Some useful questions to ask include:

- Did the plan work?
- What areas were successful and worth further investment?
- What parts of the plan came up short?
- Given the damages we incurred, what areas could use work?
- How did our service providers and systems perform?

By answering these questions and learning from the experience, your business can seize the opportunity to reflect on and improve your recovery plan before the next disaster occurs.

## Prepare for the Unexpected with Magna5

A comprehensive recovery plan is crucial to protecting your business from disaster. Avoiding these mistakes will safeguard your organization from the unexpected. Magna5 can help ensure that restoring data after a disaster is never an issue.

Our managed data backup with seamless recovery provides customers with assurance their data and network recovery are in good hands. Let our experts do the heavy lifting of managing and monitoring your data backup activities so you can bounce back quickly in the event of a cyberattack or natural disaster.

Looking to prepare for the worst? We can help. Contact us today to discuss options.

## About Magna5

Magna5 is a nationwide provider of managed services, network services, unified communications and infrastructure technology. By bringing together enterprise-class platforms from leading providers and a 24/7/365 Operations Center, Magna5 has the unique ability to leverage leading software, carrier diversity and customize solutions that drive value to customers and vendors alike.

In working with private and public businesses of all sizes, from government agencies to manufacturing organizations, small businesses and large-scale operations, we believe that focusing on the needs of our clients through a customized approach to customer service is key. With more than two decades of experience in the managed services and telecommunications industry, we've acquired the experience to understand the needs of your organization, the changing landscape of providers and diverse technologies to deliver targeted, strategic solutions that make a difference.

Whether you need managed services, security services, voice services or are looking to move to cloud-based infrastructures, Magna5 can take your organization into the future and beyond.

## CONTACT US

Corporate Office
3001 Dallas Parkway, Suite 610
Frisco, Texas 75034
844.624.6255
www.magna5global.com