Creating a Backup and Disaster Recovery Plan That Works

networksplus.com

Table of Contents

Introduction

Dear Partner,

You and your team have worked long and hard crafting your business. You have developed a strong reputation, created a suite of products and services that meet the needs of your customers and then some, and you have achieved a strong and resilient business.

All of this is what makes business continuity so critical. You would not willingly put all of this at risk. You would not intentionally leave it vulnerable. And yet, if you do not have a backup and disaster recovery (BDR) plan in place, your business is subject to these risks and responsibilities.

But don't be disheartened. Instead, be proactive. Put a plan in place. Read on to learn more how this works and how you can make sure your plan is the best it can possibly be. As always, we are here to help you navigate this and ensure your data remains safe and secure.

All Our Best,

Your Partners at Networks Plus

What Is a Backup and Disaster Recovery Plan

A backup and disaster recovery plan is your organization's safeguard against disaster or catastrophe in the event of an unforeseen incident. While the plan itself will not avert such an incident, it will give your team the roadmap it needs to stay on track and to keep afloat even during very difficult times.

The plan itself is a reactive measure, designed to be implemented if the worst should happen. With this in mind, you should develop your plan alongside a range of preventative measures designed to avoid the disaster in the first place. In this sense, the business continuity plan is a safety net for the worst-case scenario, and is designed only to be deployed if your proactive, preventative defenses are not sufficient.

Prevention is important, but no organization can see into the future with any certainty. Sometimes disasters strike. When this happens, the way your business responds is critical, both to your short-term operations and to your long-term survival. Your plan will dictate your response, and will prove crucial as you move through the hard times, and then beyond them.

Why Backup and Disaster Recovery Planning Matters

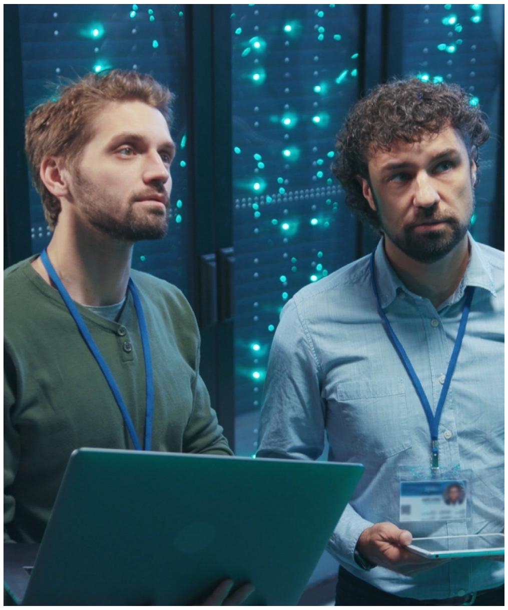
Catastrophes Can, and Do, Happen

No business owner would ever admit to being unprepared, but there is certainly an element of "well it will never happen to us" at play when it comes to business continuity. Words like "disaster" and "catastrophe" sound so serious because they are so serious, and because such events are relatively rare.

This is one reason why **5 percent of companies** report that they do not have a backup and disaster recovery plan in place, and 23 percent of companies that do have such a plan never test it to make sure that it is effective.

Despite this apparently nonchalant attitude to the potential risks, business catastrophes happen all the time. Between 2017 and 2018, 27 percent of companies reported losing revenue due to downtime. This underlines why it is so important to have a solid plan in place, should the worst happen.

"5 percent of companies report that they do not have a backup and disaster recovery plan in place, and 23 percent of companies that do have such a plan never test it to make sure that it is fit for purpose."



Your Team Members Need to Know Exactly What to Do

Your staff members know their roles, and they know these roles well. However, when your company is facing downtime, these roles shift considerably. Team members will need to take on expanded roles as they minimize risk, repair damage, and keep everything moving forward.

But it is not enough just to expect your staff to take on new duties and responsibilities. They will need to carefully manage their workloads, scaling back on existing responsibilities and executing their new duties with skill. They will need to know how to prioritize the different tasks required to get your firm back online. What's more, they'll need to do all this in a highly pressurized environment.

It is likely that your workforce is highly trained, passionate about your company, and will thrive under pressure. However, they still need to know what is expected of them, and how they will carry this out. This can only come when everyone is reading from a good-quality plan.

Vague Planning Can Cause More Problems Than It Solves

We have already touched on the discrepancy between the number of organizations that have a plan, and the number that actually test it. This is very worrying because vague and incomplete planning can land you in serious trouble.

There are a number of dangers that can arise when you only pay lip service to a plan and do not ensure that it is robust and watertight:

- Staff members do not have the metrics with which to measure progress through the crisis. Everything changes when disaster strikes, so your teams need to know what progress is being made in order to put it right. This includes a primary objective that will signify that everything is back as it should be, as well as incremental milestones along the way.

- Staff members may be confused as to which duties they are responsible for. When your plan kicks in, every angle should be covered by a specific team or individual, with some overlap to ensure success. The last thing you want is miscommunication, which can lead to wasted time and resources as tasks are carried out multiple times, or even critical tasks being missed altogether.

- Staff members may know what they have to do but not necessarily how to do it. Think about when you started out in business. You had your target in mind, but the steps to get there seemed mystifying. Remember this: Just because your team knows what it is aiming for does not necessarily mean it knows the most efficient way to achieve this.

- Under the stress and strain of disaster, the plan may begin to fall apart. An expert coach can deliver the tactics to their team, but the team needs to perform in the pressure of the moment. Make sure your plan is battle-tested so you know it will work even when the heat is on.

Your Customers Need to Be Able to Put Their Faith in You

It is not a secret that a disaster can ruin a business. You know this, your team knows it, and your customers and clients know it, too. They need to be reassured that your business has what it takes to survive such a catastrophe.

In fact, you need to go further than this. They need to know that their data is protected. They need to know that they can still access the products and services they need, at all times. In other words, they need to know that you have every eventuality covered.

And if you cannot demonstrate this to your customers? Well, don't expect them to stick around. Later on, we'll be covering how downtime can lead to loss of business and lost customers. Well, it's important to remember that even just the threat of downtime can have the same negative effects.

"Any amount of downtime is going to cost you a lot of money. Statistics from 2019 reached an average of $10,000 per hour."

Every Minute Counts

It is very difficult to put an exact dollar amount on downtime. Exact figures depend on a range of different factors, including the scale of the business, the extent of the catastrophe, the quality of the response, and even the way in which losses are defined.

One thing is certain:
Any amount of downtime will cost you — often a lot.

In fact, statistics from 2019 put the average cost at roughly $10,000 per hour. That's not a number any business can afford to ignore. Even when broken down, losses can reach hundreds of dollars per minute.

A solid plan can make the difference between responding immediately and restoring operations or delaying your response and watching losses pile up. The latter option, of course, is far more expensive.

What Can Happen if No Plan is in Place

Lost Profit

As mentioned earlier, downtime can cost businesses significantly, but the exact amount is often hard to calculate.

Consider the immediate impact of a catastrophe without a backup and disaster recovery plan: your company experiences downtime, preventing transactions and causing direct revenue loss. Customers with subscription-based services can't access what they've paid for, leading to further losses.

Then there are indirect costs. Lack of customer support during downtime may violate service agreements, resulting in fines or penalties. Product development delays can push back launch dates, reducing competitiveness. Finally, restoring operations after a disaster adds even more expense. Every one of these costs hits your bottom line.

Lost Customers

Your customers choose your business because they depend on your products and services—they genuinely need what you provide.

So what happens if you suddenly can't deliver? It's not hard to imagine the outcome.

The reality is, they will likely leave. Downtime isn't just poor service—it's a complete denial of the products, services, and support your clients rely on. Of course, this isn't intentional, and your service team may do everything possible to assist customers. But if you can't fulfill your promises, even the best efforts won't be enough.

Lost Business Reputation

The least tangible aspect of damage caused by not having a proper disaster recovery plan in place is also arguably the most severe. Your business has spent many years building a solid reputation in your industry. It would be a tragedy if you were to let something like a business catastrophe and the resulting downtime ruin that.

Let's think about where that reputation comes from.

- High-quality products and services
- Leading levels of uptime, when businesses are there for their customers
- Support that really solves customer problems and optimizes their experience
- Systems that are designed to enhance that user experience (UX) even further
- A responsible and proactive approach to security
- An ethos of putting the customer first, and working to assist them every step of the way
- Brand values that align with those of the customer

When your business experiences downtime, or a breach, because there is no plan in place, all of these elements suffer.

Some suffer more than others, of course. For example, you are still likely to have products available to customers, even if your support is offline.

However, the cumulative detrimental effect of a business catastrophe on all of these elements is going to seriously hinder your business and damage its reputation. This damage may be difficult to bounce back from.

Data Loss

From the least tangible to perhaps the most tangible risk. Data loss is a common occurrence when it comes to business catastrophe and can be the result of an innocent – but damaging – system failure, or it can be due to theft or other malicious behavior.

Your business stores and uses a high volume of data. Much of this data is considered sensitive, and may relate to personal information regarding your customers, your employees, or your partners. Some of this personal information may be used to target, defraud, or otherwise harm these innocent parties.

If you let this happen, perhaps because your backup and disaster recovery planning was not robust enough, you are going to seriously damage your reputation. Beyond this, you are going to lose a lot of customers. Beyond even this, you may find yourself on the receiving end of legal action as you did not do enough to safeguard the data in your care.

Even if sensitive customer data is not compromised, and none of the above happens, you could still find yourself facing a serious issue. This is because modern businesses need data if they are to survive. It is this data that provides the insight, the understanding, and the confidence required to move forward. Lose this data, and you lose your forward momentum, and your ability for growth.

What Staff Should Be Trained On

In order to maximize the effectiveness of your response, staff training needs to be thorough. This is what staff should be trained on.

- Knowledge of the business continuity plan so they can put it into action with no issues
- High-level communication skills so instructions and feedback can be delivered quickly
- How to watch out for emerging and evolving threats
- How to deploy data analytics to measure and assess business processes
- Performance under pressure as a disaster recovery scenario is one of the most pressurized situations in business
- Their own roles and duties – staff members get set in their ways and may not necessarily be doing their jobs in the most safe and efficient manner; regular training updates are important here
- Their expanded roles and duties – new responsibilities will emerge when the recovery plan is enacted; staff members need to know precisely how to handle this

What Should Be Included in the Plan

Staff training is a key element when it comes to combating a disaster for your business.

However, training and staff expertise still need to be supported with the right roadmap. This is where your plan comes into play.

So, what are you going to include in your plan? Where do you begin on your way to crafting the most robust response possible in the face of catastrophe?

In this section, we'll take a look at a step-by-step guide to making this happen.

Identify Essential Services/Functions

Your first step is to identify all of the services and functions that are essential to your business. Implementing a backup and disaster recovery plan will involve running your business at a kind of "bare bones" level, similar to a patient on a life-support machine. As a result, you need to know which processes are most critical to your survival.

This should include:

- All processes that achieve the minimum level of regulatory compliance for your business: You need to make sure that you are not at risk of infringing any laws, even when you are operating at limited capacity.

- All processes that provide support and assistance for clients using your products in the field: Your existing customers must take priority, and you must be able to ensure that they can continue to operate the products you have provided to them in a safe and effective manner.

- All processes that mitigate further risk and establish enhanced security: Just because your business has taken a hit does not mean you should leave it vulnerable to further damage. Continue to maintain security at all times.

- All other processes that you would consider vital to the ongoing operation of your business: It is important to prioritize here, and to score your different processes in terms of how vital they are to your business. This way, when you come to isolate different components within your architecture, you will understand the danger and risk associated with closing down each function or process.

- On the flip side of this, think about all the processes your business doesn't need: You can make this a part of the scoring technique listed above. Identify the processes that are not so important to your operation, and scale back on these if necessary as you get your business back on track.

Identify Potential Issues

Next, you need to identify any issues that may hinder your disaster recovery, or may exacerbate any existing problems. This list of issues must be exhaustive. You cannot know how to avert a disaster unless you know exactly what disaster may involve in its worst-case scenario.

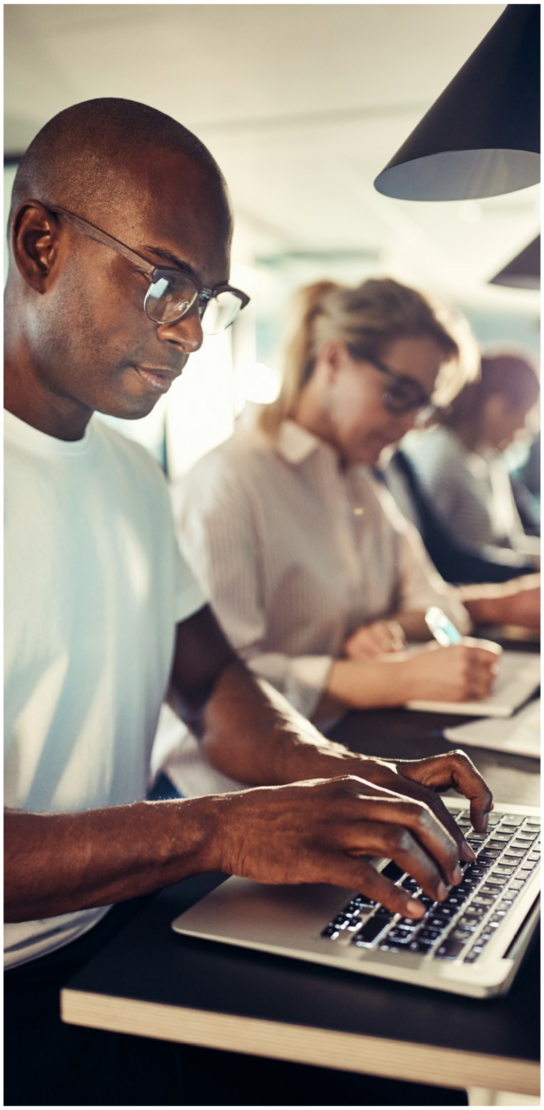
Begin to craft your business-wide risk assessment.

- Consider your data storage, gathering, and analytics network. We have discussed data loss already in this piece, but it is worth mentioning again. Data is so critical to an organization, but it is also a weak point, not to mention a potential target for thieves

- Consider key vulnerabilities. Do you use third-party contractors on a “bring your own device” policy? Do you have data that has not been backed up? Do your staff members share login credentials? Of course, you should be working to iron out these vulnerabilities, but the first step is to identify and understand them.

- Consider how threats can spread through your structure.The first part of disaster recovery is to halt the spread and to begin to roll it back. Take a look at your organizational structure and consider how you could isolate certain elements to stop the spread.

- Consider the impact of each potential problem. How long do you expect it to take before you get your business back up and running? What sort of expense and impact can you attach to the risk profile of each component? Adopt a scoring system like the ones already discussed, and get to know your priorities when it comes to risk.



Organize Your Response

Now that you know a bit more about the different processes that are at risk within your organization, as well as the different things that can sometimes go wrong, it is time to set up your time scale for response.

- Set your BDR team to work. You should make sure that you set up a dedicated disaster recovery response team ahead of time. This team will make sure that the plan is carried out completely and thoroughly.
- Begin with the most critical problems and processes identified in your scoring system.This means safeguarding your most critical processes, and mitigating your key vulnerabilities.
- Aim for isolation. It is much easier to stop a threat if you have restricted its reach to only a small part of your company. If you are trying to combat a threat without containing it, you could find yourself fighting a losing battle.
- Establish the metrics required to measure your progress. You and your team need to know what they are aiming for, and this means understanding the different metrics they will use to measure success in their efforts.

- Work through your checklist. We'll talk about your checklist below, but, fundamentally, this is the list you will work through on the way to safety and normality for your business.

- Take the steps required for transparency. It is likely that your clients and customers will not be best pleased that their data has been compromised. However, you have no choice but to disclose this to them with full transparency as the other alternatives have much worse outcomes. Decide how you will do this.

Create A Checklist

Your checklist is an exhaustive list of all the things your teams need to do to secure success when it comes to disaster recovery. This will include:

- All the duties and responsibilities each team member has

- The milestones that will be reached along the way to recovery

- The different areas of vulnerability, along with their scores and level of priority

- The different processes that need to be shut down or scaled back during recover

- The different processes that are still necessary during the recovery phase

- All the different jobs that need to be done in order to ensure a successful recovery

It is worth segmenting this checklist to ensure thorough completion. Craft different checklists for all of your different teams so they understand precisely what they need to do, with no danger of ambiguity or confusion.

Support this with a master checklist that your core recovery team works on. This master checklist will ensure that all efforts pull together to achieve the best possible results.

Review Plan

There are still a number of steps left to carry out, even after the plan has been drafted. The first step is the review. Here are a few tips to help you review your plan in the right way.

- Gain an outside perspective. When you have been working on your BDR plan for quite some time, it can be difficult to judge the plan objectively. This is why you may need to give your plan to a partner to read over, or ask teams to review plans from other departments. This outside perspective may help you to catch any errors and to refine the process.

- Be realistic. Do you have the money and resources available to carry out what is outlined in the plan? Will the measures you plan to take realistically save your business? Consider this with care.

- Streamline the plan. As we have touched on above, every minute your organization spends offline translates to a huge loss of revenue. It also puts your business at risk of irreparable reputational damage. Make sure your plan is as streamlined as possible so your route to recovery is a swift one.

- Consider every eventuality. The last thing you want is for critical elements to fall through the cracks in your plan. Make sure all of these elements are included, and leave nothing out.

Revise, Test, and Update the Plan

The initial review is just the first step to properly appraising your plan. Threats to your business are evolving all the time, which means that your recovery plan needs to be evolving, too, to keep pace with these threats, and to stay one step ahead of the game.

- The first thing you need to do is battle test your plan. Devise different drills based on the different risks that your organization might face and then put your team, and your plan, through its paces. Make time to do this regularly so you know your plan is truly up to the task.

- Derive data from these tests and use this data to improve your plan going forward. When you start to implement these practical tests, you will begin to see inefficiencies and other failings in your process, and you will begin to know how to put these right.

- Make sure that your team is staying on top of all threats as they evolve and grow. New threats emerge all the time, and your plan needs to be able to respond to this shifting landscape. Give this duty to one or more of your disaster recovery core team members, and stay on top of the situation.

- Hold regular meetings with your implementation team. This way, you know the plan is fully up to date and ready to go as and when required. Make sure that the plan is a living, evolving entity that is robust enough to meet the needs of the here and now, but flexible enough to continue to meet these needs tomorrow.

Final Thoughts: Work With a Managed Service Provider to Help Fill the Gaps

Ensuring that you have covered every possible angle when crafting your business continuity plan is not easy.

Unfortunately, there is no room for error. If your plan is incomplete, or somehow not ready for action, this can leave you and your business horribly exposed. To put it simply, this is something you cannot afford to get wrong.

This is why working with a managed service provider can offer such an advantage This is an organization with:

- The expertise required to craft and implement a winning disaster recovery plan
- The ability to work with your company to really get to know what you need, and then put that into action
- The time and resources required to ensure full focus on the task at hand, and to make sure the process goes without a hitch
- The experience required to ensure no base is left uncovered within your business continuity plan

Consider working with a managed service provider as they can make the difference between a plan that is robust and fit for purpose, and one that is simply unsuitable.

Are you interested in securing your business future? Would you like to secure peace of mind and effectiveness by working with a trusted MSP?

Reach out to us today to find out more or to enlist our services at consulting@networksplus.com.

1800 Kimball Ave.
Manhattan, KS 66502

800.299.1704
consulting@networksplus.com
networksplus.com

NETWORKS PLUS