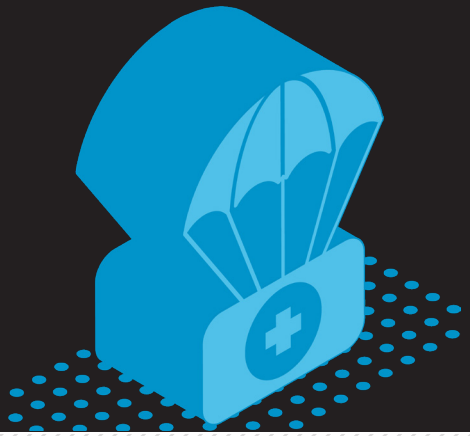

IF YOU WAIT, IT'S TOO LATE

GET AHEAD OF DISASTER

TALK TO AN EXPERT

INTRODUCTION

Far too many businesses wait until a cloud disaster strikes to realize the necessity of a disaster recovery plan. At this point, it's often too late to take action to prevent a majority of the financial loss incurred. According to IBM, the average data breach costs American companies upwards of $8 million.

While having a plan in place to prevent cloud disasters doesn't guarantee a company will be spared the headache and stress of an emergency, it can exponentially reduce the cost by almost half when the unthinkable happens. Companies with fully-fledged security automation in place saved on average $3.58 million, according to the same IBM study.

Some cloud disasters take significant time to contain as well, sometimes nearly a year. Think of the cost of manpower alone that it will take to come back from that, especially if a company is stuck in reactive mode trying to assess the damage.

The good news is that most cloud disasters don't simply materialize out of thin air, and there are elements that your company can control in order to significantly reduce your risk of damage from natural disasters, data breaches, cyber-attacks and more. By understanding the forms cloud disasters can take, creating a dynamic recovery plan, and leaving room for adjustments, your company can be well on its way to preventing.

THREE OUT OF FOUR COMPANIES ARE UNPREPARED FOR A CLOUD DISASTER

MAIN TYPES OF CLOUD DISASTERS

While it's not possible to prepare for every single eventuality, it is possible to get close. Understanding the most common cloud disasters can help companies construct multi-faceted plans to account for the most probable threats to their cloud. The first step to being prepared is to know what to look for.

1. Natural Disasters

Consider the potential for natural disasters, like hurricanes, tornadoes, wildfires, and floods, to impact your company. No part of the United States is immune to such events, and they can lead to power outages, equipment damage, and building operation disruptions. Assess your facility's location, structure, and vulnerability to local weather conditions. If your area faces flooding risks, safeguard your hardware from water damage and ensure your provider's facility can maintain operations during adverse conditions.

2. Hardware and Software Malfunctions

Sometimes things simply stop working. This unfortunate reality can sometimes feel unavoidable. The network goes down or part of your hardware breaks, and like dominoes, every problem leads to another. In a normal year, the average SMB loses $1 million to downtime, according to the Manifest.

The most important element to look at here is the redundancy of your network. This can buy your team significant time to isolate and address the issue without major service interruptions for your customers. Look at your failover rates. Are you seeing long stretches where the network is down, with no way to get it back up? Are your customers affected by the network failing? If either of these are happening to you, make note of these pain points to address when you are developing your cloud disaster recovery plan, and make it a serious discussion point with your off-premises provider.

3. Human Error

Human error is one of the leading causes of cloud disasters. Whether or not the attack was malicious, these honest mistakes or intentional actions can cost your company millions. While it's hard to think of your own employees being dangers, it's important to maintain a realistic view of the threats at hand. People like an angry team member or a new hire who hasn't completed their training can, knowingly or unknowingly, contribute to a major security problem.

Do you have safeguards in place to prevent your own employees from being the catalyst of a catastrophe? Things like multi-factor authentication, access controls, and surveillance monitoring systems can all mitigate the risk of human error. If you're not sure whether human error prevention should be a part of your plan, think again. When it comes to compliance standards that will further offset exposure in this area, ISO 20000-1 is critical.

4. Cyber Attacks

This is the cloud disaster that most quickly comes to mind. Cyber-attacks encompass phishing, DDoS, and data breaches. This is the bogeyman of cloud disasters, since they can sneak up without warning, through the smallest cracks in your company's cloud infrastructure. "At this point, the most likely and most damaging cloud disaster threat is ransomware," says LightEdge CSO, Michael Hannan. "Safeguards against ransomware should be a priority when developing your disaster recovery plan."

Do you have your customers' information locked down? Are you confident in your ability to protect your network from a DDoS attack? When you and your team are planning for cyber-attack recovery, be sure to bring up the option to proactively provide protection against malware and DDoS attempts so you can get ahead of the threat.

WHY YOU NEED A CLOUD DR PLAN

Every business should plan for the worst, even if it seems unlikely or is uncomfortable to think about. Cloud disasters can strike at any time and with little-to-no warning, so it's best practice to plan early and well for how your company will respond, whatever form the disaster may take.

Retain Customer Trust

Trust is one of the hardest things to build and among the easiest to lose. Customers and clients are the reason employees get up and go to work each day, and it's vital to continue to provide high-quality customer service, even in the midst of a disaster. Being available for support, making deliveries or conducting meetings should all be possible, no matter what's happening behind the scenes. If you lose customers because you cannot provide adequate service, the effects of your cloud disaster will reach far into the future, since 58% of customers are unwilling to continue doing business with a company after a negative experience. Cloud disasters, if poorly handled, have the capability to cripple your customer service practices as well as decimate your customers' trust in your ability to keep their information safe. Even years down the road, you may be struggling to regain your reputation, depending on the scale of the disaster. Do you have your customers' information locked down? Are you confident in your ability to protect your network from a DDoS attack? When you and your team are planning for cyber-attack recovery, be sure to bring up the option to proactively provide protection against malware and DDoS attempts so you can get ahead of the threat.

Cost of Being Unprepared

Even though it's played-out, the saying is true: time is money. Take a look at all the ways a cloud disaster could impact your bottom line:

- Each minute of downtime costs an average of $5600. Over time, those losses can be devastating.
- Cloud recovery can take up to 280 days to fix completely, taking up the most of a fiscal year on simply containing the situation, let alone rectifying lost trust or compensating customers for damages.
- Lost revenue as customers can't access your platform or portal that could eventually lead to loss of their business after a hit to your reputation.

There are also a few more unexpected areas where you could lose money after a disaster, depending on the industry:

- Legal costs, depending on the nature of the business and accompanying regulations.
- Replacing employees that leave after poor disaster recovery.
- Loss of stakeholder support & stock values plummet.

Ensure Business Survival

The sad truth is that a cloud disaster can be the kiss of death for many companies. Between the massive loss of trust and significant financial hit, moving forward might be impossible. The good news is that it doesn't have to be this way with appropriate cloud disaster recovery planning. By building out a comprehensive disaster recovery plan, you can take some of your power back and ensure your company's future success.

WHAT SHOULD BE PART OF YOUR PLAN?

1. Account of All Types of Disasters

Once again, make sure you understand the categories of disasters and are making plans for all the forms they can take. Plan for multiple contingencies so you can take early action and nip the disaster in the bud before it becomes a five-alarm emergency.

2. Business Continuity Planning Checklist

How will your company continue to function in the midst of a cloud disaster? This is essential for coming out well on the other side of a crisis. As you build out your own effective business continuity plan, be sure to include the following provisions:

Identify all emergency personnel in relation to each type of incident. Gather their contact information and place at the top of the plan so you can get in touch with them quickly and aren't wasting time leafing through the document for an appendix.

Once you've identified your emergency personnel, establish a flow of communication and cadence of updates. How much information do you need before you post a notification? When will you meet to discuss important steps? Outline a communication pattern that works for you, so nobody is left in the dark for too long.

Ensure adequate resources for recovery. It's always good to have an emergency fund, on-call personnel, and a system that can be backed up. Disaster recovery is not the time to cut costs.

Find a safe, secure place for your team members to continue to conduct business until after the disaster passes. Make sure you have all the equipment needed for your essential functions, such as connectivity, printers, and space for everyone to meet.

Figure out your IT recovery plan while prioritizing critical systems. The plan should include strategies for returning the office to productivity as well as restoring enterprise software. Go for the options with the least amount of downtime.

All team members should be aware of their roles and responsibilities before, during, and after a cloud disaster. Train employees early and often and be sure to update models as roles change.

Set a reminder to update information that is likely to change, such as mission-critical infrastructure, vendor contact information, organization charts, and manufacturing components.

Once you think you have a plan, walk through it with other team members with the intention of finding weaknesses. Everyone deserves a seat at the table when it comes to disaster recovery planning. You may also consider doing disaster simulations to really put these plans to the test in a realistic scenario.

3. Think You're Ready? Test Again.

Companies should provide their teams with testing and different exercises to evaluate each business impact and its corresponding recovery strategy. Be sure to document the results and implement necessary changes. Perform multiple tests to see how policies hold up and compare and schedule time to review and update your plan regularly. We recommend quarterly or annually. If it's not up-to-date, it's no use in the event of a cloud disaster.

> "A DISASTER RECOVERY PLAN SHOULD BE REGULARLY UPDATED, REVIEWED AND TESTED," SAYS HANNAN. "A GOOD PLAN IS NOT WRITTEN BY A SMALL GROUP. YOU WANT TO HAVE INVOLVEMENT FROM ALL KEY STAKEHOLDERS AND FUNCTIONAL LEADERS."

AFTER DISASTER STRIKE

Evaluate What Went Well

Give credit where credit is due. Recognize employees who went above and beyond in recovery efforts and take note of what worked well for your company and customers. Find ways to expand on successful elements and see what lessons you can carry over into your plan for the next time.

Evaluate What Went Wrong

This is the part of the process that is most important. After you made it through to the other side of a cloud disaster, take a look at areas that caused the most friction or the areas that took the longest to resolve. After these areas are identified, sit down with the team to brainstorm ways to improve the process, just in case your company is hit with another attack, natural disaster or software malfunction. Constant evolution of your disaster recovery plan is necessary to keep up with emerging trends in cybersecurity, software and more.

Get Ahead with Prevention

Prevention is always the best policy for cloud disaster recovery. Prevention strategies act a bit like window screens. A few gnat-sized human errors may get through, but you may be able to avoid a massive falcon of a DDoS attack landing on your network. It's about controlling what you can on the front end in order to have more time available to deal with what you can't control once the crisis is actually on your doorstep.

Your risk mitigation plans are just as valuable as your disaster recovery plans. Look at all the potential risks that you encounter on a daily basis. Here are just a few to get started:


Single-factor authentication on customer transactions


Lack of education about endpoint security for remote workers


Frequent power outages due to inclement weather

There is typically a way to mitigate most risks by adding layers of security and education to your existing policies. Take a moment to write down your pain points and come up with ways to move toward a proactive risk mitigation strategy.

DISASTER PREVENTION OPTIONS

Prevention is always the best policy when it comes to risk mitigation. You can significantly reduce the cost and losses associated with a cloud disaster by investing in services and solutions that prioritize compliance, security, and excellent failover. Not every cloud disaster is one hundred percent preventable, but anything you can do to minimize your risk of having one is a step in the right direction.

Compliant Cloud Choices

As more companies shift to the compliant cloud, more options become available, depending on your business needs. The three main types of cloud storage, public, private and hybrid all come with their own unique advantages and disadvantages so be sure to thoroughly review your business's needs before making your selection.

Private clouds have long been labeled as the superior choice, often at a premium price point. With a private cloud, companies expect total control, data protection, and high performance. When weighing their options, users are quick to believe that public clouds are more affordable than private, but there comes a point where a private cloud solution can be a less expensive option for enterprises.

The new kid on the block is the hybrid or multi-cloud, which offers a customizable way to leverage cloud technology. While there are many ways to make hybrid cloud work for you, one of the most common ways it is done is through on-premises environments with connections to public cloud. Despite its murky definition, hybrid cloud utilization is growing in popularity. As enterprises explore hybrid clouds more, they're learning that implementation of a hybrid cloud solution can be difficult due to the nature of the transition.

Data Protection Services

It is essential to revisit your data protection and security strategy. As cyberattacks and malware become more complex every day, it may be time to consider investing in data protection services to layer up on security measures and restore some peace of mind.

Data protection services help back up and protect your data, working to eliminate accidental data loss and quickly recover from cloud disasters. To get the most out of your investment, opt for a data protection service that also focuses on applications, not just data and servers. The importance of data protection increases as the amount of data that is created and stored continues to grow. Start protecting your data early so you're prepared for your company's future growth.

Colocation

Colocation is a highly secure data center facility where equipment, servers, space, and bandwidth are available for businesses to purchase. Companies who chose to invest in colocation providers' host servers, experience higher security and guaranteed uptime. Most companies are not able to own and operate their own data centers, so they use a colocation facility to house their own infrastructure.

Colocation hosting improves uptime, cuts costs, and boosts the quality of customer service. Colocation can take a company's existing server and move it from their own storage to the colocation provider's data center. Utilizing colocation services allows you to focus exclusively on managing your own operations and meeting goals, while lowering the impact on your IT budget.

DRaaS

Disaster Recovery as a Service (DRaaS) reduces the time it takes to return applications to production. DRaaS can fill in the gaps for small and medium-sized businesses that may lack the necessary expertise and manpower to build, test and revise an effective disaster recovery plan.

DRaaS providers restore the backup, and often restore the infrastructure immediately including most of your critical elements, such as databases, files, applications, and software. For infrastructure that has been custom built and is difficult to maintain, DRaaS gives you the ability to back up your own infrastructure on a replicated server. Large businesses that depend on their data also consider DRaaS to ensure the continuity and integrity of their infrastructure. Facilities built to Tier III standards and talented engineers are ready to accommodate your business' requirements.

YOUR DISASTER RECOVERY NEEDS: LIGHTEDGE IS PREPARED

Feeling overwhelmed by the challenges of preparing for a cloud disaster? LightEdge understands the importance of your peace of mind. In today's IT landscape, where cloud and on-premises storage converge, safeguarding your applications and data demands specialized solutions that can rise to the occasion.

At LightEdge, our unwavering commitment is to our clients. We're dedicated to ensuring the security of your IT operations, critical applications, and data, no matter the threat. We provide the technology and resources tailored to meet your Recovery Time Objective (RTO) and Recovery Point Objective (RPO) requirements, swiftly restoring your operations to full productivity.

Our comprehensive suite of disaster recovery solutions is designed to maintain uninterrupted performance for your IT operations and mission-critical systems during cloud disasters. The reliability of your business IT is paramount, regardless of your company's size. Everything hinges on the reliability and accessibility of your technology, delivering vital information precisely when you need it.

At LightEdge, redundancy is our core principle, ingrained in all our data centers. We go beyond the standard, offering Hybrid Solution Centers that provide a full range of high-speed, secure, redundant, local cloud services and managed gateways to public clouds through our fortified facilities.

Connect with one of our disaster recovery experts to explore our services further or schedule a private tour of our data center facilities. Our team of disaster recovery, colocation, and business continuity specialists is ready to address all your inquiries and concerns. Your peace of mind is our priority.