Whitepaper

DartPoints

A Modern Approach to Disaster Recovery and Business Continuity: What You Need to Know

From natural disasters to cyberattacks to pandemics, emergency situations can arise with little or no warning and often with extreme consequences. That is why business leaders understand the importance of emergency preparedness to mitigate interruptions and keep their companies operational no matter what.

Disaster recovery (DR) is a completely different beast today compared with ten, five, or even two years ago. The truth is, the amount of downtime a company or application will accept at this point is near zero. A single outage that causes hours, or even minutes, of downtime can be detrimental. Cloud-native applications and deployments are driving recovery time objectives (RTOs) and recovery point objectives (RPOs) to almost unbelievable lows. The speed of light will not allow for the level of RPOs that some companies are demanding, and requirements simply can't be met in all geographies.

Plus, gone are the days when DR was synonymous with copying data from point A to point B and bringing virtual or physical machines online during a disaster. Now, DR is so mission critical that the industry is building applications with it built right in. The bottom line is: DR has never been a more important boardroom conversation, and it's more sophisticated than ever.

A Quick Note on Definitions

Companies put disaster recovery and business continuity (BC) plans into effect to help minimize the repercussions of crises and the resulting unexpected downtime. Although these concepts are often used synonymously — and they're linked, to be sure — there are differences between the two that make it important for business leaders to consider each separately.

An easy way to distinguish one initiative from the other is to look at when each takes effect. Business continuity requires you to keep operations functional during an emergency and immediately after. Disaster recovery focuses on how you respond after the emergency has concluded, when the business is undergoing the necessary steps to return to normal operations. DR is an IT-specific practice that falls under the much broader BC plan, which also encompasses employee safety, work locations, communications, and more.

3 Questions to Consider for DR / BC Planning

Recognizing the difference between the terms is just the first step in a potentially overwhelming process, but it does not need to be overly taxing. By answering some key questions, you can determine what your next steps will be when a disaster occurs — before there's even one on the horizon.

#1: What are your risks and how do you respond to them?

The first step is to figure out what kinds of risks will impact your company, and to determine what your initial steps are for each type of risk. These first steps will likely be different — after all, you'd react differently to a fire than you would to a theft — but should all follow the same pattern? If your workplace is inaccessible to your employees, you should ask yourself:

- How and when will you contact them about the disaster?
- Where will your employees go when a disaster occurs, if appropriate?
- How will you transport your employees to a safe location?
- How will the plan work in the real world?

Identifying some of the specific risks that your business faces and then formulating and testing a response plan for those risks are the first steps towards an overall recovery plan. Business continuity is all about keeping your employees safe, your data secure and your operations running, so establishing an immediate disaster recovery plan sets a solid foundation for your additional continuity planning efforts.

#2: Where will your employees work if the building's safety is compromised?

Your employees are the heart of your business, so ensuring they can continue working after a disaster is crucial. If you need to find an alternate physical location, keep in mind that you may not need to house every employee in a company-owned office location. You'll want to consider who can work from home, which is a quickly growing crowd following the COVID-19 pandemic.

Maybe you have a backup office, call center space, or a room at your data center that can be used as additional workspace. Regardless of your solution, consider your options for a secondary workspace when putting together your business continuity plan.

#3: Where are your data and equipment located?

Your continuity plan should always take the data element into account to truly be complete (and ultimately successful). This means considering where your data, applications, and servers are located, and assessing whether changes are needed in order to be as prepared as possible.

A comprehensive continuity plan will either include a colocation or a Disaster-Recovery-as- a-Service (DRaaS) solution. Both Disaster Recovery solutions continually replicate data from a primary site to a secondary site, whether it be a data center or other facility. This helps ensure two things:

- Your data, applications and equipment are not at risk of being damaged or destroyed when your location is impacted by a disaster.
- Your employees will continue to have access to all of the data and applications they need, even when working out of a secondary location.

When it comes to your critical IT equipment and data, it is always important to ensure that your servers are running at a location that is safe against a wide range of disasters, but it is especially important when you are creating a business continuity plan.

Choosing a DR Provider

Arguably, the single most important DR-related decision for your company — beyond prioritizing your DR strategy to begin with — is choosing the right disaster recovery provider. Your IT infrastructure requires a consistent approach to keep your business secure and operational, and given the rise in cybersecurity threats and natural disasters in recent years, enterprises that partner with technology experts are a step ahead. Therefore, finding the right DR partner is the most critical step to ensuring your company has an effective, reliable plan in place. Here are some key factors to consider in selecting the provider who best meets your requirements:

Security

The impact of losing data is almost unimaginable, and ever-evolving threats require elite data protection solutions beyond essential compliance. Choose a provider who engineers comprehensive security, backup, and data recovery solutions that are designed to prevent attacks and to help you discover and recover from any attacks that do occur.

Cloud Coverage

Recovery cloud (DRaaS) designed to complement your cloud or physical environment is a key component of your disaster recovery plan. Look for a provider that not only helps you identify your mission-critical servers and space requirements, but also ensures your data is available when you need it, with hourly replication, bi-annual testing, and flexible RPOs and RTOs. High-performance cloud that couples best-in-class infrastructure with the highest level of care and customer service results in an ultra-reliable, geo-diverse cloud.

Support

Rather than paying an entire department to handle the burden of managing backups, overseeing cybersecurity, and responding to your ever-changing storage needs, a disaster recovery provider offers comprehensive and cost-effective support. Look for a provider that offers a variety of enterprise data center managed services centered around helping you store, access, and protect your valuable data. 24/7/365 on-site support provides additional security and peace of mind.

Location

For ideal disaster recovery, the data center that houses your secondary and tertiary backups should be easily accessible to someone on your team, yet more than 30 miles away from a major metro area. The building should be fully redundant and highly secure, of course, but that's table stakes for a DR facility. Additionally, during the site selection process, operational leaders should carefully evaluate locations based on climate, environmental conditions, and the probability of a natural disaster.

Finding the right provider for your needs depends on your specific requirements, but there are elements that should always be considered when choosing your ideal provider, including:

- Industry Experience
- Cloud-Based Disaster Recovery Services
- Colocation-Based Disaster Recovery Services
- Power Redundancy
- Network Redundancy
- Environment Redundancy
- Security Redundancy
- Extra Amenities

Conclusion

Business continuity planning will ultimately determine how well your business can continue functioning after a disaster, so the more thought and preparation you put into that plan, the better off your company, your employees, and everyone who depends on them will be.

About DartPoints

DartPoints is the leading digital infrastructure provider enabling next-generation applications at the edge. The company's unique suite of services, "Digital Next," combines digital infrastructure and hybrid cloud with DartPoints' edge internet exchange offering (BridgeIX $^{\text{SM}}$) and edge high-performance computing solution (Liquid Edge$^{\text{SM}}$).

By weaving together cloud, interconnection, colocation, and managed services, Digital Next enables edge ecosystems for enterprises, carriers, and cloud and content providers. DartPoints is building tomorrow's distributed digital infrastructure while serving today's cloud and colocation needs — and helping to bridge the digital divide.

To learn more about DartPoints' DR solutions, visit:
https://dartpoints.com/solutions/managed-services/disaster-recovery/.