US SIGNAL®

A GUIDE TO DR PLANNING

The Whats, Whys and Hows

201 Ionia Ave, Grand Rapids, MI 49503 | 866.2.SIGNAL | ussignal.com

Table of Contents

v2.0
9.28.17

Introduction

With all the news stories about data breaches, cyber-attacks, and storm-related power outages — and their negative effects on the companies impacted by them — one would think every organization would have a disaster recovery (DR) plan in place. A survey by the data protection firm Zetta says many don't, supporting what numerous other studies have shown: many companies do not make DR a priority.

The Zetta survey of 403 IT professionals reported that 40% said their organizations don't have a documented DR plan. Of those companies that have a plan, only 40% test it at least once a year. Fifty-four percent said their company had experienced a data outage of at least eight hours in the past five years, with power outages, hardware errors, human errors, virus/malware attacks and data corruption as the biggest reasons for such interruptions.

The reasons for not having a DR plan in place vary. In one survey, 39% of the respondents said they were currently developing a DR plan while 29% said they simply hadn't gotten around to it yet. Lack of funds was cited by 26%, while 20% felt their current backup systems would suffice. Other studies have shown that the leadership of many organizations think the chance of a disaster affecting their operations is minimal and are willing to take the risk.

The fact is disasters can and do happen. They can be costly, and potentially put companies out of business. There's no time like the present to get DR planning underway to help your company mitigate the effects of potential data loss and downtime. In this eBook, we'll cover several topics you should consider when developing a DR plan.

BC and DR: There is a Difference

Before developing a DR plan, it's important to understand how DR fits in the overall scope of business continuity (BC). In both the IT and business worlds, the terms "business continuity" (BC) and "disaster recovery" (DR) are often used interchangeably. While the concepts behind them are related, BC and DR do have different meanings. Understanding those differences is essential in preparing for disruptive events that have the potential to bring IT operations — and the businesses they support — to a halt.

BC: Staying in Business

BC refers to the management oversight and planning involved with ensuring a business operates with minimal or no downtime during and after a disruptive event. The word "during" is important because you always need your business to continue operating normally even during a disaster. Any downtime has the potential to result in lost revenue, lost business and more.

Not all data or IT systems are necessary for business operations. The BC plan will specify which are. This will drive network bandwidth requirements and the use of specific replication technologies. Critical applications may require a geographically load-balanced back-up with instant failover powered by high speed links. Less critical systems may suffice with periodic snapshots running on slower connections.

DR: Recovering Your Data

DR is a subset of BC. Its focus is on getting essential data and IT systems back up and running after a disruptive event. The emphasis here is on "after" as you want your data saved somewhere so it can be recovered after the business-disrupting event.

Note that the data is not accessible during the disruptive event. It must first be recovered, and the speed at which it is recovered is dependent on the planning, resources and processes that are set forth and tested in the DR plan.

Beyond Definitions

Both BC and DR are essential to any organization that expects to stay in business even if a disaster — manmade or natural — strikes. Knowing the differences between the two concepts is important, but creating, implementing and testing plans for each is what matters most.

Compliance Factor

BC/DR planning requires companies to determine what data, applications and IT resources are critical to their continued operations and, ultimately, their survival. Combined with an assessment of potential risks, this knowledge enables them to put strategies in place for minimizing business disruptions and data loss, and quickly returning to “business as usual.” However, keeping a business going isn’t just in the interest of the business, and this is where the compliance factor comes into play.

The government knows that keeping the flow of goods and services going so tax revenue is generated is an economic necessity. That’s why it extremely interested in helping to ensure that the private sector, as its own operations as well, remain up and running. Most businesses should be as well. Yet, they either put BC/DR planning on the proverbial back burner, refuse to invest in it altogether, or make only half-hearted attempts to put a plan in place. Government regulations help these companies make BC/DR a priority since failure to comply can result in expensive penalties.

Several organizations — like the International Organization for Standardization — also have developed standards and guidelines to help companies ensure their continued operations and to protect the interests of those with which they do business.

The Language of Compliance

It can be a lot for businesses to keep track of when it comes to doing what’s required. Understanding the terminology and hierarchy makes it a bit easier.

At the highest level of compliance requirements are laws. There’s no option for not complying. Laws must be followed, and failure to do so can results in harsh penalties. HIPAA, which applies to many companies within the healthcare industry, is a good example. Next are regulations. They carry the weight of law, so there are penalties for non-compliance. Industry standards represent best practices. Following them is strictly voluntary so there are no fines if you don’t. However, failure to adhere to them can have other consequences, such as not having a viable BC/DR plan in place. Then there’s the matter of certification, which is a process that companies undergo to verify they meet specific industry standards. Some certifications may have a BC/DR requirement involved.

Your Compliance To-Do List

Stay current with the laws and regulations specific to your industry. Review them carefully to understand any BC/DR requirements they may contain. Seek professional advice from compliance experts. In many cases, they can also provide guidance on necessary certifications, third-party audit requirements and other information.

Consult the variety of resources available regarding BC/DR best practices. You’ll find a number of them at the Department of Homeland Security’s web site: https://www.ready.gov/business/implementation/IT and at the web site for the Disaster Recovery Journal: http://www.drj.com/resources/dr-rules-regulations.html.

If you outsource any portion of your BC/DR efforts, work with vendors that have compliance experts of staff and that, themselves, are compliant and hold pertinent certifications.

Backup and Replication

Few like to admit it, but the “language” of DR planning can be confusing. Is data backup and data replication the same? If you have one, do you need the other? What about data archival? Where do things like encryption and deduplication fit in?

The Safety Net: Backup

A backup is a copy of data used as a safeguard against unexpected data loss and application errors. If you lost your original data, you can use the backup to make it available again. This differs from data archival, which protects information that isn’t needed for day-to-day business but must be retained for a long period — often for compliance purposes.

Backups entail making copies of data files at intervals. It could be hours or days between the copies, depending on your business requirements. The copies are saved to an off-site physical hard drive, tape, disk or to a virtual tape library (VTL). Or, you can use cloud-based backups that allow you to backup data from any physical or virtual infrastructure, or Windows workstation, to a cloud service. You can then access your data any time, from anywhere.

Some providers also offer backups as a managed service, handling everything from remediation of backup failures to system/file restores to source. The techniques used will depend on the type of data you’re backing up and how convenient you want the recovery process to be. Other than storage media costs, backup is relatively inexpensive. It may take time for your IT staff to retrieve and recover the data, however, so backup is usually reserved for data you can do without for 24 hours or more. Application performance can also be affected each time a backup is done. There are various ways to manipulate data to improve backup and recovery speeds, data security and reduced bandwidth requirements, including:

- **Compression.** Various schemes can be employed to shrink the source data so it uses less storage space.
- **Deduplication.** This eliminates multiple copies of the same thing, and can be applied at the file level, on raw blocks of data, on a server before any data moves to the backup media or at the target storage device.
- **Duplication.** Backups can be duplicated to a second set of storage media. This allows for rearranging the backup images to speed up recovery, or to have a second copy at a different site or on another storage medium.
- **Encryption.** Encryption uses algorithms to change the form of data to protect it during backup and recovery. Only those holding an encryption key can read the data.

Real-Time Replication

Data replication is like backup in that it copies and moves data to another location. The difference is that replication copies data in real- or near-real time, so you have a more up-to-date copy. Replication is usually performed outside your operating system, in the cloud. Because a copy of all your mission-critical data is there, you can "failover" and migrate production seamlessly. There's no need for wait for backup tapes to be pulled.

Replication copies every change, even if the change resulted from an error or a virus. To access data before a change, the replication process must be combined with continuous data protection or another type of technology to create recovery points to roll back to if required.

Replication costs more than backup, so it's often reserved for mission-critical applications that must be up and running for business operations to continue during any business interruption.

Key Considerations

Back up and/or replication alone don't make for a comprehensive DR plan for most companies. However, both tactics can play a role in DR. The following questions can help you determine what that role should be.

- How important is the data on your systems? Do you need to back it all up or is there some that won't matter if it's lost? If specific data must be backed up, when and for how long?

- What type of information does the data contain? Is it subject to regulatory requirements? Does it need to be kept private? Does it need to be kept for a specific period? How often will you need to access it? (The answer to the last question will help you determine if data archival may be required.)

- How quickly do you need to recover the data? Can you go without it for a day or maybe even a week? Do you need it right now to keep business going? If that's the case, replication may need to be part of your strategy.

- Do you have the equipment to perform backups? If you're doing your own backup, you'll need hardware. If you don't already own it, you'll need to purchase it.

- Do you need to store backups off-site? In almost all cases, the answer is yes. The bigger question may will the off-site location be one you manage or belong to a vendor? Will it be a physical data center or the cloud?

Your answers to the above questions may also help you determine if you should do your own backups or outsource. Handing off the responsibilities to a vendor not only frees up your internal resources. It also can offer benefits such as reduced capital expenses (no equipment to purchase) and access to data protection best practices.

Traditional or Cloud-based DR

There's traditional DR and cloud-based DR. Which makes the most sense for your organization?

An Overview of Traditional DR

Traditional DR can be as simple as backing up data to disks or tapes and manually taking them off-site where they can be stored until needed. (Refer to the previous section "Backup and Replication.") At the other end of the complexity spectrum is maintaining a complete remote data center where data and applications are replicated on dedicated backup servers and storage, and data, applications and systems configurations can all be restored.

At first glance, backing up data to disk or tape seems like a good option for keeping data safe until it's needed in the event of a disaster. However, backup software and/or the backup media can fail. The disks or tape on which backups are saved aren't free. The person responsible for backing up data can make mistakes. The time between data backups can result in lost data.

In addition, tapes or disk stored on-site can be lost if a disaster strikes. Storing backups at an off-site location solves that problem, but a safe off-site location costs money. It also takes time to physically transport media to an off-site location, as well as to retrieve it and pull the information off. Data backup also doesn't do anything for applications and system configurations — both of which are integral to disaster recovery.

That's not to say backup doesn't have its place. Use cases including keeping a copy of everything from the least important to most critical data for compliance, and for pinpointing recovery of anything ranging from an employee's emails for e-discovery to a deleted file from five years ago. But backup, by itself, doesn't make for a strong DR solution.

Most companies going with traditional DR opt for a hot, warm or cold facility.

- A hot site is a fully equipped data center with servers that can be online within hours. It's expensive but a great way to minimize downtime and data loss.
- A warm site provides basic infrastructure but requires some lead time to prepare servers and go online. It costs less than a hot site but the lead time required may not be worth it.
- A cold site has the basic infrastructure needed to run a data center, but little else. Equipment must be brought in and configured, which can take weeks to be operational. It's the least expensive of the options if you can afford the down time.

Any of the aforementioned DR solutions require that the facility be located so that any regional disaster doesn't affect both the production and DR sites. However, data takes more time to travel longer distances. If you need synchronous replication to meet your RPO or RTO, the DR site will need to be in closer proximity to your production site. You'll also need staff on hand to help with the DR solution implementation.

Cloud-based DR

Cloud-enabled DR delivers several advantages over traditional DR, such as reduced capital expenses because it eliminates the need for investing in a remote DR facility. Ongoing operating expenses are lowered because you don't have to pay to power and cool remote equipment. Capacity and performance can be allocated on demand, so you only pay for the resources consumed. Because the cloud is designed for remote management, it speeds up recovery. Compared to on- or off-site tape-based DR, such capabilities can make routine testing more practical, and help ensure the DR service works when needed.

In addition, the cloud makes warm site DR a more cost-effective option. Backups of critical servers can be spun up in minutes on a shared or dedicated host platform. With SAN replication between sites, hot site DR also becomes a less expensive option. SAN replication provides rapid failover to the DR site with very short recovery times, offering the capability to return to the production site when the DR test or disaster event is over.

Cloud-based DR also offers the ability to finely tune the costs and performance for the DR platform. Applications and servers that are considered less critical in a disaster can be tuned down with less resources, while still assuring that the most critical applications get the resources needed to keep the business running through any business disruption or disaster.

If you are concerned that cloud-based data backup could open your data streams to breaches from a third party or because of other customers residing in a given data center, there's no need to worry. Many cloud service providers (CSPs) build high-level security features into their clouds. Typically, CPSs that are audited to meet the requirements of the Healthcare Information Portability and Accountability Act (HIPAA), Payment Card Institute Data Security Standard (PCI DSS), and other regulations or industry standards, employ security best practices to help ensure data safety and integrity.

The DRaaS Option

Cloud-based DR can be delivered "as a service," and is referred to as "Disaster Recovery as a Service" or DRaaS. DRaaS entails a service provider charging a recurring fee for replicating and hosting a company's physical or virtual servers and providing failover to a cloud environment hosted by the provider if a manmade or natural disaster occurs.

As a managed service, DRaaS — at least as offered by the more reputable service providers — includes proactive monitoring and handling of threats courtesy of the DRaaS provider, as well as DR best practices that many companies don't have the time or expertise to handle. That includes coordinated data restoration testing and frequent alignment of minimum recovery point objectives (RPO) and recovery time objectives (RTO).

Among the reasons that DRaaS is often preferred over other cloud-based DR options, such as cloud backups, is time. With cloud backups, you can restore data, but it can take hours. You must download the application files from the cloud based on your most recent backup, rebuild, and then compile the data or application. If the application runs, you know you have restored a clean copy. If not, you must go back to the next recent backup and go through the process again.

With a DRaaS solution, you can quickly stand up and failover to a DR environment. Then with a few clicks you can fail back. Data can be restored in minutes. If you consider the cost of downtime for SMBs — approximately $10,000 per hour according to many estimates, it's easy to see why you'd want your data restored as quickly as possible — especially for mission-critical applications. (The costs can run even higher for enterprises.)

Of course, some companies may be able to tolerate a little more downtime than others — at least for their less essential applications. With that in mind, more service providers are offering DRaaS "tiers," which allow you to select the service level that works best for your budget and needs. You can provide the same data protection for both mission-critical and non-mission-critical applications, but pay based on recovery priority and the resources required.

DR Plan Testing

DR testing enables you to identify potential issues or gaps in your DR plan so you can take corrective action now. There are various DR testing methods with some more "invasive" than others. Here are some of the more common ones:

Walk-through - Your DR team goes through each step of the plan verbally to identify weaknesses or gaps. It's the least disruptive of the various methodologies, but you don't really get to see the various components of your DR plan in action.

Table-top/Simulation - More in-depth than a walk-through, this typically doesn't affect day-to-day business operations. It is scenario-based, focusing on specific types of disasters or business disruptions. It may involve role-playing and actual physical testing of alternate sites and equipment, as well as coordination with vendors and others.

Parallel – With a parallel test, recovery systems are built/set up and tested to see if they can perform actual business transactions to support key processes. Primary systems still carry the full production workload.

Full-interruption - In this test, actual production data and equipment are used to test your DR plan. This has the potential to disrupt business operations and can be time-consuming. However, it can also be extremely worthwhile by demonstrating any gaps or problems in your plan.

Sandbox – Many third-party companies that offer disaster recovery as a service (DRaaS) solutions "sandbox" or partition virtual machines so testing can be performed without affecting production servers.

Set the right expectations for "testing success." Even if a test fails, it may be considered successful. After all, its purpose is to identify weaknesses during testing rather than in an actual disaster.

Testing Frequency

DR plans are complex, with lots of moving parts. Infrastructure, business processes, and personnel change, and every change must be integrated into the DR plan. Doing so, however, creates opportunities for something to fail or a mistake to occur. Testing at pre-determined intervals can help ensure that plan changes are accounted for and that they don't affect how a DR plan works when executed. Even if you're working with a third-party provider, make sure that DR testing is not a one-time thing.

Testing Follow-up

After each DR test, it's critical to document successes, failures, and other information to improve the DR plan so your staff is ready for the next test — or an actual disaster. A DR plan is only as good as the last test, and it's the lessons learned during testing that enable recovery success in an actual disaster scenario.

The Outsourcing Question

When it comes to DR planning, you don't have to go it alone. In fact, in may be a good idea to outsource if you lack the time or in-house resources and expertise. There are several service providers out there that specialize in DR solutions. The key is to find one that can best meet your needs. Here are some things to consider when looking at potential DR service providers:

- **Knowledge and interest.** The service provider should know about the industry you're in and the challenges and opportunities that could impact your DR plan. The provider should also want to learn about your business, your goals and business requirements, your back-up and recovery challenges, your data and application profiles, and growth expectations.

- **Ability to deliver.** Can the provider achieve your RPO and RTO for your most critical data, applications and business operations? Is the provider willing to put a guarantee in its service level agreements (SLAs)? Does it have references who can vouch for its follow through and performance?

- **Compliance.** Operating physical and cloud infrastructures according to compliance requirements requires a continuing commitment to staying current with the ever-increasing industry and government regulations; investment in physical plant and technology to assure compliance; and training the workforce to understand and carry out their duties accordingly. Look for providers with a portfolio credentials, such as SSAE-16, PCI DSS, and HIPAA/HITECH. Don't take a provider's word that it holds specific certifications or undergoes compliance audits. Ask to see relevant documentation.

- **Security.** It would seem that security and compliance would go together, but don't assume that if you have one you also have the other. Find out about the scale and scope of a provider's logical and physical security policies, programs, testing and auditing.

- **Support.** The best DR service providers will have 24/7/365 technical support. They'll also have skilled experts to fully manage server and storage recovery at all times.

- **Geographically diverse data centers.** The provider should have data centers strategically placed so as not to be affected by the same single disaster, as well as to have the power, communications, networking, redundancy, staffing and security to sufficiently meet your requirements. If possible, tour at least one of the provider's data centers.

- **DR testing.** Ask any potential DR service provider to explain in detail its testing processes. That will include what is tested, how it is tested, and how often tests are conducted.

You'll likely have several other questions, depending upon your organization's specific needs and requirements. Assemble all your questions before meeting with prospective DR service providers so you'll be better prepared to assess their capabilities.

DR Planning Starts Now

There's no time like the present to get your DR plan started. Whether you'll be working with a third-party company or are taking on DR planning on your won, the following steps will get you off to a good start.

Assess Your Risks

Start your DR planning efforts with a risk assessment. (If you've gone through the steps for building a business case for DR to present to management, you may have already gone through some or all of these steps to create a risk profile.) A risk assessment examines the vulnerability of your IT assets to events that can cause downtime — including cyber-attacks, internet outages, and natural disasters. Geographical location and weather patterns can come into play here. For example, if you're in an area at risk for flooding or a location with limited transportation access (which could prevent employees, as well as emergency services, from accessing your site), your IT operations could be at risk.

Look at all possible disaster scenarios, as well as weaknesses that could make your IT assets susceptible to damage from a hazard. This could include things such as deficiencies in building construction or being in a multi-tenant building (a fire or broken water pipe in the suite next door could put your business as risk.)

Inventory Your Assets

Now take stock of your IT assets that could be affected. Get input from others within your company as "shadow IT" could have introduced essential data and applications without the knowledge of your IT department.

Identify any application and system dependencies. For example, you may have a commerce application that incorporates an authentication server, a product database, a database or an inventory system from a partner or supplier. You can't successfully recover this application without ensuring that the applications on which it depends are recovered as well. Most likely you also have hardware or equipment dependencies such as an email server may that depends on a storage array, which in turn depends on specific network equipment.

Conduct a Business Impact Analysis (BIA)

Determine the operational, financial and reputational effects to your business if your IT assets were not available. Consider the costs associated with downtime including, but not limited to, lost revenue, delayed sales, regulatory fines, customers who move on to your competitors, and brand damage. This will help you to calculate how much downtime your business can tolerate.

Identify the resources required to maintain your business operations, if possible. Then establish an order of priority for restoring business functions and related data or applications. Don't forget about any compliance requirements.

Define Your Recovery Objectives

Once you understand the potential costs of downtime and the likelihood of threats, set recovery objectives for each of your critical applications.

- Recovery point objective (RPO). Your RPO tells you how much time from the point of the outage you can afford to lose. Your RPO will determine the frequency with which you'll need to replicate data from your production site to a DR site. If your RPO for an application is one hour or less prior to disaster, you'll need to replicate data at least hourly. If you can't afford to lose any data, ever, you'll need to implement synchronous replication for that application. In other words, you'll need to have your data written to a DR site at the same time it's being written at your production site.

- Recovery time objective (RTO). Your RTO established how quickly you need to have data or applications back up and available after disaster. This answer is less about data loss, and more about having the application or data available. This will vary widely depending on the application and/or data and who uses it. Your internal data warehouse may need to come back online in several hours, whereas a customer-facing website may need to be back up immediately.

Pick Your Strategy

Now comes the fun part — reviewing and evaluating different data backup, replication and recovery strategies. Will tape backup work or is disk backup the better option? Should you keep your data backups on site or move them to an off-site facility? If you go with off-site backup, do you want a facility that is equipped with everything you need to get recovery started immediately even if you are paying for everything even when it's not in use. Or, does it make more economic sense to bring in the equipment needed for data recovery at an off-site facility only when needed, even if that means the total time required for recovery could be quite long.

Be Prepared for Anything, Any Time

Ensuring your business can continue operations and recover critical data and applications if a disaster strikes is essential to your organization's survival and success. The strategies are out there. It's a matter of choosing the ones that are right for your business, incorporating them into a plan and testing that plan to ensure your company can weather the storm or any other disaster — any time.

A Few Final Words

There's much more to developing, implementing, and testing a DR plan than can be covered in a single eBook. However, the information provided in this publication should get you off to a good start.

If you'd like additional information, or need a place to start in terms of looking at DR service providers, contact US Signal.

US Signal can work with you to devise a customized DR solution drawing from a broad portfolio of data protection and managed security solutions. US Signal's Professional Services team can also assess your current DR plan and make recommendations for best practices that can make it more effective.

For more information, phone at 866.2. SIGNAL or by email at info@ussignal.com

v2.0
9.28.17