IT Disaster Recovery

What to know. What to do.

US SIGNAL®

Table of Contents

Introduction

From ransomware attacks to hurricanes, disasters can and do happen. When they do, they can take out IT systems and bring businesses to a screeching halt – or, at the very least, disrupt business operations. Either way can be costly, and put companies out of business.

That's why DR plans – and the DR solutions at the heart of them – are no longer "nice to haves." They're "must-haves" that help ensure organizations can weather any kind of disaster, mitigate potential downtime or other damage, and keep their businesses operating.

In this eBook, we'll cover several topics that are essential in evaluating DR solutions and creating or modifying a DR plan.

Gain a Solid Understanding of DR

When it comes to disaster recovery (DR) planning, the first thing to do is to educate yourself on the basics. This includes terminology, strategies, technologies and best practices.

Learn the differences between DR and business continuity (BC), replication and backup, failover and failback, recovery time objectives (RTO) and recovery point objectives (RPO), and traditional and cloud-based DR options.

Take the time to get up to speed on current and emerging trends - in terms of DR threats and risks, and DR solutions.

Evaluate Your Current Approach

Review how you currently handle DR and backup. Who is responsible for and takes the lead on DR matters? Do you have a formal DR plan in place?

Is your organization employing industry best practices for DR? Are you accounting for all your data, applications and IT infrastructure? Are these tactics meeting your recovery point objectives (RPO) and recovery time objectives (RTO)? Have you tested these tactics to make sure they work the way you think they should work?

Are you confident that if a manmade or natural disaster struck, your company could continue doing business or at least mitigate issues enough so you could be back online quickly without disrupting your business operations?

If there are deficiencies in what you're currently doing, or you don't have any kind of DR or backup plan in place, determine if you have the in-house expertise and available resources to fix the situation. If you do, get on it. If not, seek out a service provider that can help.

Whether or not you have a formal DR plan in place, the following pages provide information to help you in creating or updating one.

Inventory Your IT Assets

Inventory your data and applications. What do you have? Where is it? Who needs it and how often? Who has access to it?

Get input from others within your company as "shadow IT" could have introduced essential data and applications without the knowledge of your IT department.

Also identify all the mission-critical infrastructure required to keep core business operations up and running. Don't forget about essential resources such as power and cooling.

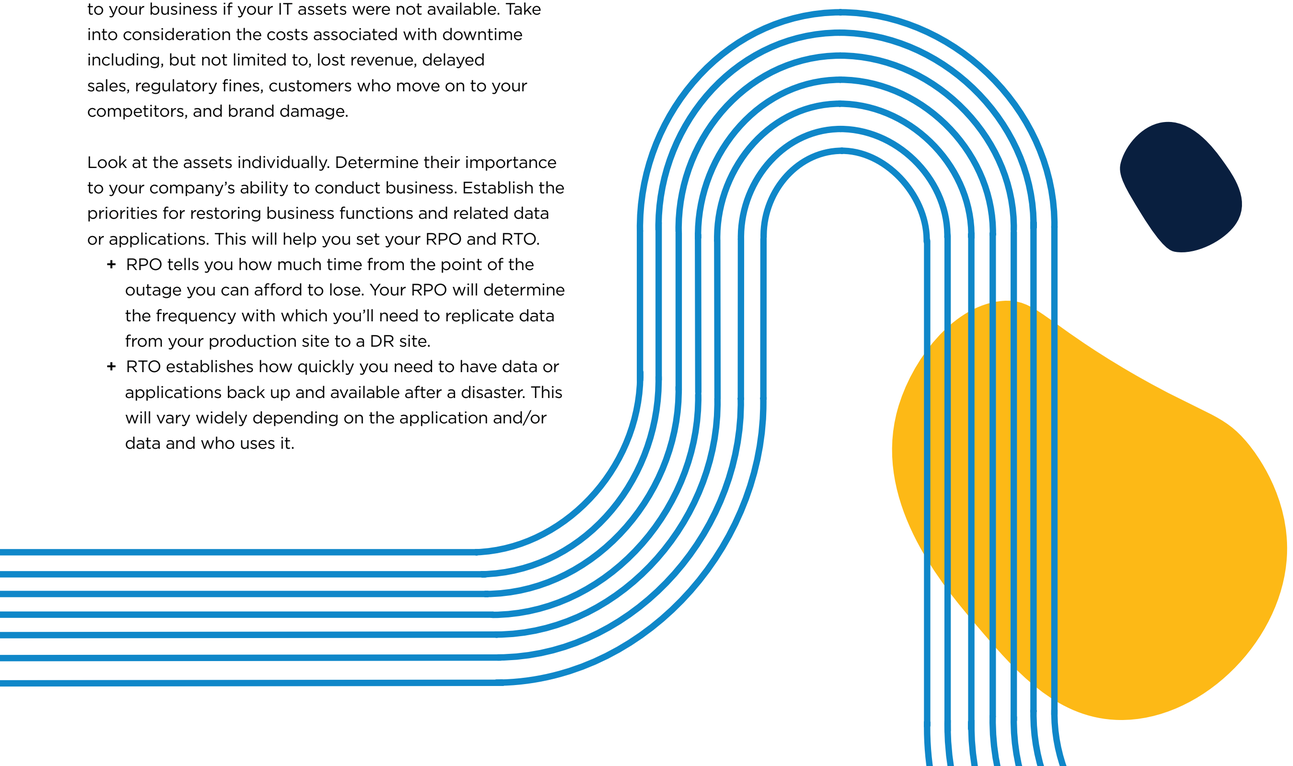
Even if you have a DR plan in place, it may not be covering the entire breadth of your IT systems. Map out all application and system dependencies. For example, you may have a commerce application that incorporates an authentication server, a product database, a database or an inventory system from a partner or supplier. You can't successfully recover it without ensuring that other applications that depend on it are recovered as well.

Conduct a Business Impact Analysis (BIA)

Determine the operational, financial and reputational effects to your business if your IT assets were not available. Take into consideration 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.

Look at the assets individually. Determine their importance to your company's ability to conduct business. Establish the priorities for restoring business functions and related data or applications. This will help you set your RPO and RTO.

+ 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.
+ RTO establishes how quickly you need to have data or applications back up and available after a disaster. This will vary widely depending on the application and/or data and who uses it.



Conduct a Risk Assessment

List the various scenarios and events that could affect your IT assets and cause downtime, data loss or corruption, or otherwise disrupt your business operations. Rate the level of risk from probable to unlikely.

Consider categorizing them as follows:

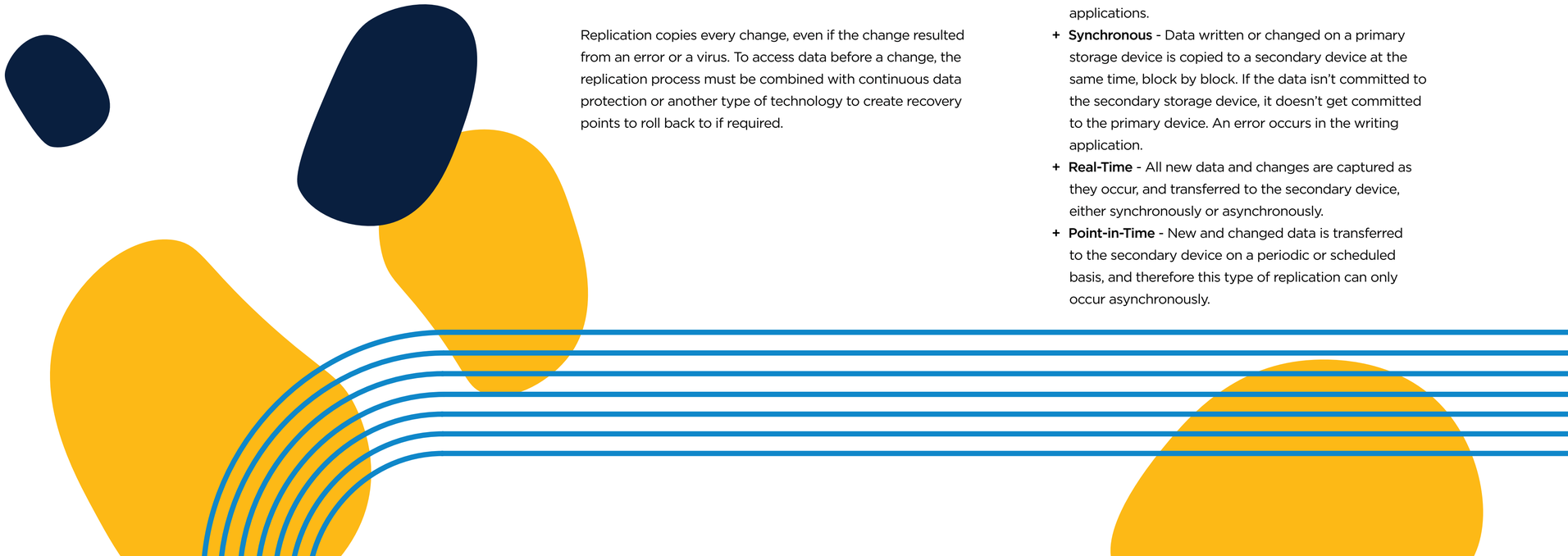
+ **Natural disasters** - For example, if you're in an area where tornadoes are common or roads are frequently flooded during storms (which could prevent employees and emergency services from accessing your site), your IT operations could be at risk.
+ **Technology/equipment failures** - This could include anything from hardware and software failures to system overload and cut cables.
+ **Cyberattacks** - Sophisticated ransomware and phishing attacks are among the most dangerous and common causes of IT downtime.
+ **Human-related** - This includes human errors, as well as internal threats that can result things like corporate espionage and employees that misplace devices, resulting in unauthorized access to an organization's network.
+ **Miscellaneous** - This cover the random events that can put an organization at risk for IT downtime. For example, squirrels and birds have been known to cause power outages.

Conducting vulnerability scans of your IT systems and third-party assessments of your IT maintenance and security processes and technologies can help reveal the potential for various types of risks. You can also learn from case studies of other companies that have endured and/or gone under due to various types of disasters.

Review DR Strategies - Backup

Among the DR strategies to evaluate are backups. They can include:

+ **Disk or tape backup** - With this type of strategy, backups are scheduled and entail making copies of data files at intervals. It could be hours or days between the copies, depending on business requirements. The data copies are saved to a physical hard drive, tape, disk or to a virtual tape library (VTL), which are kept offsite. The techniques used depend on the type of data you're backing up and how convenient you want the recovery process to be.
+ **Hybrid backup** - This entails backing data up on a local device and in a secure offsite data center or the cloud for redundancy. You always have a secure local copy of your data as well as the offsite copy. Systems are backed up to the local device first, so you don't have to worry about the replication to the data center or cloud affecting the performance of your systems or Internet connection.
+ **Direct-to-cloud** - With this option, you bypass the local device and send your data directly to the cloud. You're still backing up your data to a remote data center, but without the local copy on site. Depending on your Internet speeds and specs of your machines, these backups could take much longer. See page 16, Cloud Backup, for more information.



Review DR Strategies - Real-time Replication

Data 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.

There are four common types of replication:

+ **Asynchronous** - Data written or changed on the primary storage device is sent to the secondary storage device, but the timeliness and/or successful completion does not impact the primary storage device or the writing applications.
+ **Synchronous** - Data written or changed on a primary storage device is copied to a secondary device at the same time, block by block. If the data isn't committed to the secondary storage device, it doesn't get committed to the primary device. An error occurs in the writing application.
+ **Real-Time** - All new data and changes are captured as they occur, and transferred to the secondary device, either synchronously or asynchronously.
+ **Point-in-Time** - New and changed data is transferred to the secondary device on a periodic or scheduled basis, and therefore this type of replication can only occur asynchronously.

Backup and Replication Considerations

Back up and/or replication both can play roles in DR. The following questions can help you determine what those roles should be.

+ How important is the data on your systems?
+ What type of information does the data contain? Is it subject to regulatory requirements? Does it need to be kept private? 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? 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 need to store backups off-site? 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 these 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.

Review DR Strategies - Disaster Recovery Sites

Another option for DR is maintaining a 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. Your choice here will be between a hot, warm or cold disaster recovery facility.

These DR solutions require that the facility be located so that any regional disaster doesn't affect both the production and DR sites. If you need synchronous replication to meet your RPO or RTO, the DR site will need to be in closer to your production site. You'll also need staff to help with the DR solution implementation.

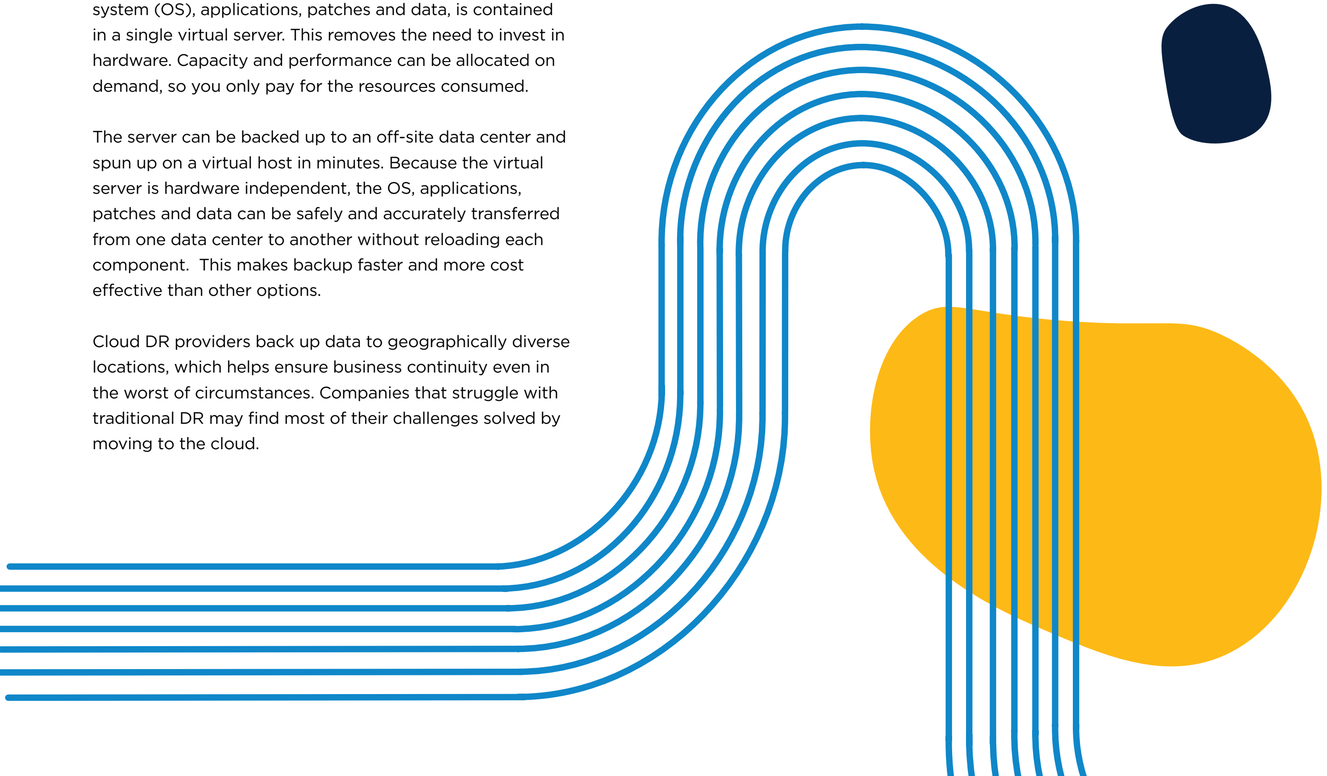
+ **Hot site -** This is a fully equipped data center with servers that can be brought online within hours of an adverse event. Choosing a hot site for DR is expensive, but it's also a great way to minimize downtime and data loss and ensure business continuity.
+ **Cold site -** A cold site includes the bare-bones infrastructure needed to run a data center. You supply your own equipment and configure it, which may take weeks to bring online. It's the least expensive of the options, but the most work.
+ **Warm site -** 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 negate the financial benefits.

Review DR Strategies - Cloud-Based DR

With cloud-based DR, the entire server, including operating system (OS), applications, patches and data, is contained in a single virtual server. This removes the need to invest in hardware. Capacity and performance can be allocated on demand, so you only pay for the resources consumed.

The server can be backed up to an off-site data center and spun up on a virtual host in minutes. Because the virtual server is hardware independent, the OS, applications, patches and data can be safely and accurately transferred from one data center to another without reloading each component. This makes backup faster and more cost effective than other options.

Cloud DR providers back up data to geographically diverse locations, which helps ensure business continuity even in the worst of circumstances. Companies that struggle with traditional DR may find most of their challenges solved by moving to the cloud.



Review DR Strategies - DRaaS

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, as well as DR best practices that many companies don’t have the time or expertise to handle.

By employing true continuous data protection, a DRaaS solution can offer an RPO of a few seconds. Applications can be recovered instantly and automatically — in some cases with an SLA-backed RTO of minutes.

In addition, DRaaS solutions use scalable infrastructure, and allow virtual access of assets with little or no hardware and software expenditures. This saves on software licenses and hardware. Because DRaaS solutions are managed by third parties, your internal IT resources are freed up for other initiatives.

Review DR Strategies - Cloud Backup

Cloud backup is off-site backup to a third-party service provider or to your own cloud infrastructure using cloud enablement technologies or on-site appliances. Multi-site data redundancy is integral to cloud backup as a local data copy can live in an on-site appliance, while the enablement technology replicates data to your service provider or your data center.

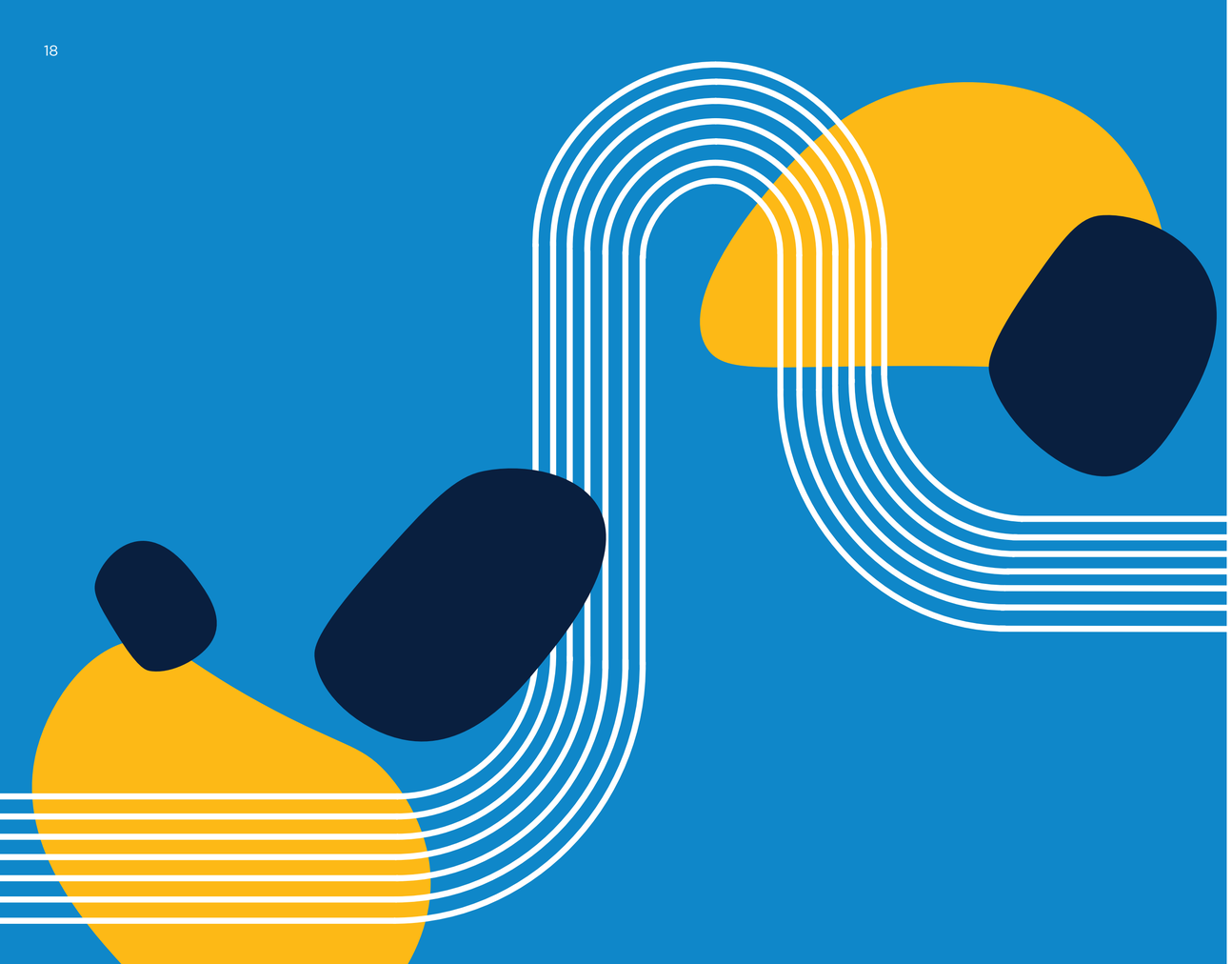
The appliances and enablement technologies continually run in the background of IT operations, eliminating some of the issues associated with manual IT processes. There are no tapes or disks to buy or refresh, and no need to spend hours each week physically managing backups or transporting tapes. However, sufficient bandwidth is required to support off-site replication. This may mean investing in network optimization or replicating less data.

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) and other regulations or industry standards, employ security best practices to help ensure data safety and integrity.

Select a DR Provider

If you've decided to outsource some or all the responsibility for your organization's IT DR plan, including going with a DRaaS solution, the next step is to select a DR partner that can meet your needs. These partners may be managed service providers (MSPs), companies that specialize only in DR, cloud service providers (CSPs) that offer DR services, among others.

+ Ask for and check references. Has the DR company successfully met SLA requirements? Is it easy to work with and does it provide prompt service?
+ Make sure any company you consider has the required expertise in regulatory compliance, security services, and in working with the platforms and applications you use.
+ Consider factors that may be specific to the type of DR solution you choose. For example, the company's ability to provide geographically diverse facilities will be a major factor if your DR plan includes primary and secondary physical sites.
+ Can the provider achieve your RPO and RTO for your most critical data, applications and business operations?
+ Ask any potential DR service provider to explain in detail its testing processes.
+ Seek out providers that will help with installation and initial data seeding, as well as provide 24/7 support.



Test, Update and Test Again

Tests should be conducted at least annually, the results evaluated, and plan updates made as needed. There are various DR plan testing methods, each with its own advantages and disadvantages. Among them:

+ 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 methodologies, but you don't get to see the various components of your DR plan in action.
+ Table-top/Simulation - This is scenario-based, focusing on specific types of disasters or business disruptions. It may involve role-playing and physical testing of alternate sites and equipment, as well as coordination with vendors and others.
+ Parallel – With a parallel test, recovery systems are 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 - 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 demonstrate any gaps or problems in your plan.
+ Sandbox – Many third-party companies that offer DRaaS solutions "sandbox" or partition virtual machines so testing can be performed without affecting production servers.

Don't be surprised if during the testing process, failures occur. It's better to identify the problems during testing rather than during an actual event. Determine what needs to be done to correct any gaps or problems uncovered by the test and who needs to perform the required actions. Follow up to make sure the corrective actions are completed.

Your Next Steps

The information contained in this eBook is only meant to be a starting point in terms of creating a comprehensive, effective DR plan – or modifying an existing one. There are numerous other considerations; many will be specific to your organization's unique business requirements. Others may be driven by changing risks – both physical and cyber.

If you're interested in learning more about DR solutions or in creating or updating a DR plan, US Signal is here for you. We offer a variety of DR and data protection services, including DRaaS options, backup and replication. We can work with you to build a flexible, cost-effective solution tailored to your needs.

Call 866.2.SIGNAL or email info@ussignal.com

Spotlight on US Signal's **DRaaS for VMware**

US Signal's DRaaS for VMware is a cloud-based DR solution powered by VMware's vCloud Availability replication solution and US Signal.

- Familiar VMware tooling and no third-party software layers for simple integration
- Pay only for what you use — VMs protected, and storage consumed
- Support for partial or full failover and failback with native VMware vSphere replication
- Built-in SSL encryption provides security from your site to the clou
- No VPN needed because connectivity is built in between the tenant and US Signal vCloud-powered cloud environment
- One-click on-premises implementation with a virtual appliance
- Flexible RPO from minutes to hours
- Instant RTO as quickly as replicated VMs are powered on

Test Drive US Signal DRaaS for VMware for 30 Days Free. No Obligation.

+ vmware®
US SIGNAL®