Disaster Recovery | Planning Ahead

A Practical Guide to Establishing a Proper Technology DR Plan

CyberFortress™
The Recovery People

cyberfortress.com
855-223-9322
sales@cyberfortress.com

Table of Contents

Chapter 1:

Defining the DR Planning Process

In today's world, there are two certainties every business must come to grips with. The first is that outages – whether due to human error, natural disasters, or something in between – are going to happen. **In the past 12 months, 71 percent of small businesses, 79 percent of mid-size businesses, and 87 percent of large businesses all experienced one or more outages.** The second certainty is your employees, contractors, partners, supply chains, and customers all expect that your business is available 24/7.

Thus, the importance of Disaster Recovery (DR). But DR isn't just about recovering data and servers; it's about resuming business operations. In most cases, any kind of material disruption requires far more complex a response than simply running a restore job within your backup software.

So, there needs to be a DR plan in place. One that is the result of analyzing what data, applications, systems, networks, data centers, and workloads make up operations that are critical to the business. One that comprehensively defines what, where, how, and by whom recovery should take place. And one that identifies and addresses the gaps that exist in IT's current ability to recover.

This eBook is designed to help you focus in on what processes to follow to build a proper technology DR plan. While high-level, our intent is to provide you with practical guidance on how to build one and what should be included.

In this chapter, we'll discuss what the DR planning process should look like, what preliminary steps you will take.

DR Experts: CyberFortress and Veeam

Without a properly planned executed DR strategy, the DR itself is full of risk.

CyberFortress and Veeam together provide organizations with expertise and automation to ensure DR plans are successful with as little manual overhead at possible.

Look for insights from CyberFortress and Veeam throughout this eBook!

3 Reasons Your DR Plan Needs a Plan >

Before the Plan

The first step isn't to jump right in and start planning. The plan is going to require IT to disrupt several parts of the business including employees, IT staff, and budget – and that's just to build the plan. A DR plan is an agreement of how the business will act should a major disruption occur, so it's necessary to take a few steps prior to beginning to build the DR plan.

Step 1: Get Executive Sponsorship

DR isn't cheap. It also is very important – particularly when the business operations have ceased. So, at a minimum, you're going to need to have executive buy-in to both approve the plan and to address any gaps found during the planning that require budget, staffing, outsourcing, Executive sponsorship can exist in the form of an individual from the executive team or an entire steering committee, depending on your organization's makeup.

Insights: Leveraging Expertise - Most IT professionals have limited exposure to recovery efforts, with very few ever having to perform a recovery of an entire environment. And while recovery on paper looks like it's going to work, the reality is, without experience in preforming recoveries, even the most seasoned IT pros won't know what may go wrong. CyberFortress and Veeam together provide decades of experience in DR – from software solution designed specifically to automate even the most complex recovery, to experts ready to lend a hand or take the lead on particularly challenging recovery effort.

Step 2: Establish the DR Team

Those involved with building and executing a DR plan are not all going to be from IT. Yes, of course, IT plays the most significant role in the recovery of a business' technology, but there are a few more roles from within the organization that need a seat at the DR table:

- **Executive Oversight** – While execs probably won't have much to add when discussing DR technology or processes, they will want a seat at the table to ensure what you're planning will meet the business' objectives. You won't hear them talking much, but you will need to look over and get a nod from them every once in a while.
- **DR Coordinator** – this is someone from IT who will oversee the actual recovery process in the event of a disruption. They will also oversee any recovery simulation testing.
- **Recovery Expert** – this may be someone within the organization, or an outsourced partner with large numbers of recovery efforts under their belt.
- **Recovery Advisors** – these can be department heads, line-of-business owners, application owners, or tech-savvy users that IT can lean on to provide guidance around how the recovered parts of the operation need to work in order for the business to become productive.

Download: DR Team Roles checklist

Step 3: Have a Plan to Update the Plan

There will, no doubt, be changes needed in the DR plan. As, people, business goals, and technologies change, it will be necessary to keep the plan current. As you walk through the rest of this eBook, you're going to be inundated with a lot of very specific parts of the DR plan that will have you thinking in many directions. So, it's important to keep in mind that you need to establish how, when, and by whom the plan will be maintained. Without doing so, the plan will quickly diminish in value; the plan's value is found in its continual current state, ready to address the existing needs of the business. Consider the following:

Regular reviews – Depending on the criticality of the business functions impacted by a given DR plan, reviews can be as frequently as quarterly, or as infrequently as annually.

Review process – Does your plan need to be reviewed by the DR team lead? By the entire team? Should you include executives, or line-of-business owners? You should both determine this and document it in the plan.

The remainder of this eBook will focus on the steps necessary as part of building a DR plan.

This includes:

- **Performing a Business Impact Analysis**
- **Performing a Risk Assessment**
- **Define DR plan goals**
- **Building and testing the DR plan**
- **Addressing gaps identified throughout the process**

Insights: Partner-Based Review - Staying on the theme that IT's plan is still written by a group of individuals that may have never preformed a recovery of the magnitude being planned. So, it's a good idea to include a partner with specific expertise in DR to review your plan both when it's written and when it is updated. CyberFortress has experts on staff who have led the charge on hundreds of recovery efforts. They can provide guidance on where the plan may go wrong, as well as offer suggestions on how to better execute the plan to ensure a fast, accurate, and consistent recovery result.

Chapter 2:

Starting with Impact and Risk

Most IT professionals, when asked about Disaster Recovery (DR), tend to run right to the technology (as it's what they know best) and can easily come up with a plan to recover a given server, application or data set. But truly recovering from any kind of loss – regardless of whether it's a loss of data, location, or something in-between – it's important to not start with technology, but instead start with the business. When a disaster strikes, the business suffers. And, to fully understand how to mitigate this loss of operations, it usually can't be as simple as "just restore everything"; there isn't enough time, bandwidth, processing power, etc. to get everything back up and running at the same time. So, it's necessary to prioritize around the business and the impact a disaster can have on it from the perspectives of operations, compliance, legal, and process. Without first assessing the impact and risk, it's impossible to design a DR plan that appropriately mitigates these negative influences on business continuity. There are two best practices commonly held when considering building a formal DR plan.

Blog: These are performing a Business Impact Analysis and a Risk Assessment.

Business Impact Analysis (BIA)

The BIA should assess all business functions, processes, and their dependencies that will need to be recovered. Generally, a BIA uses the work flow of your business as a guide to help identify the potential impact of business disruptions resulting from any kind of loss of operations. At this point, you're not concerned about specific disaster scenarios; the focus is simply on how a loss of any given part of the business would impact operations. Generally, the BIA is comprised of a set of uniform questions that will be used to interview application, department, and line of business owners across the organization. They should be uniform in design to ensure responses can be equally measured against one another. BIAs should start with the business and work towards technology (e.g., start with the Sales Department and not with your CRM application).

BIA Questions

The following is an example set of questions that will help derive an understanding of the impact any loss of data, systems, applications, or locations will have on the organization.

1. **What business functions do you rely upon on a daily basis?** This question will help you establish a line from the business to the underlying technology. Answers may be in terms of specific data sets, systems, applications, or locations. Ask the following questions for each of the answers provided in question 1.

2. **How much data can you afford to lose (in minutes/hours/days, as is applicable)?** This helps to establish a recovery point objective (RPO) for each of the relied upon parts of technology.

3. **How much time can you afford to be without this business function while still being considered acceptable?** This helps to establish the recovery time objective (RTO) for a given backup set.

4. **What is the maximum tolerable period of disruption for this business function?** This helps to establish a wort-case scenario for a given business function.

5. **Are there any legal or compliance requirements for this business function?** It's important to know if there are any outside influences on RPOs and RTOs for a given data set.

The result of the BIA is a set of interview answers that should provide you with an idea of which business functions are, in general, important to the business. It would be helpful to use the results of the BIA to establish a fundamental prioritization of functions based on the responses. This will help the Risk Assessment be more impactful, as it can be focused on those business functions that the organization obviously cannot do without.

Download: Business Impact Analysis Worksheet

Risk Assessment

Now that you have a baseline understanding of what is important to the business and how various kinds of business disruptions will impact the organization's ability to operate, it's time to apply that analysis by assessing the risk that will exist in various disaster scenarios. The BIA will include certain assumptions (for example, it's conceivable that each application owner or line-of-business owner is going to assume their workloads and processes are the most important), so it's imperative to systematically run those assumptions through a scenario-based assessment to accomplish a few goals:

- Measure the risk associated based on the impact that loss has on operations and your customers using a combination of types of loss (data, system, application, process, location) and potential outcomes of that loss (e.g. the loss of your organization's CRM application used by Sales).
- Prioritize the severity of specific business disruptions. The prioritization will be based on both how the disruption impacts operations and on how likely the specific loss is (e.g., a hurricane is likely if the business is in Miami, but not an issue if in Ohio).
- Analyze the gaps that exist between the people, process, and technology that delivers some form of DR today with what's needed based on the BIA.

Blog: 3 Reasons Your DR Plan Should Be Based On Risk

Insights: Having Proper Recovery Objective

Both RTO and RPO are commonly held as the defining standards for what the recovery needs to look like. But they also serve as the guideline for how backups are to be generated. A 15-minute RTO requires backups every 15 minutes and may cause backups to need to be taken at an image level or even use replication instead of backups.

CyberFortress and Veeam together provide a number of backup options that are based on your specific recovery objectives – from standby images, to replication to the cloud, to fast image-based backup and recovery.

Insights: Mitigating Loss with DRaaS

Many organizations leverage on-premises resources for both operations and recovery. While this methodology can address a loss of data, system, or application, it cannot address losses in the internet connectivity, nor location.

CyberFortress and Veeam together offer a cloud-based DRaaS solution that ensures any loss can be remediated within minutes, allowing employees, contractors, partners, and customers alike to quickly access needed services, applications, and data.

Preforming Risk Assessment

The following is an example set of steps you can use to perform a risk assessment using your completed BIA. This process should be focused on whether the existing DR strategy can address each disruption scenario for a given business function.

ASSESSMENT STEPS

1. **Identify Potential Disruption Scenarios**
   This can include previous disruptions, natural and man-made risks, and environmental and facility risks.

2. **Establish Probability of Occurrence**
   For each disruption identified in step 1, determine the likelihood of this disruption happening.

3. **Assess Potential Impact**
   Apply the BIA to each of the scenarios, assessing how business operations will be affected.

4. **Report on DR Gaps**
   The outcome of applying the BIA to the disruption scenarios should reveal shortcomings in your current DR efforts.

The result of the assessment is that you have a very detailed and prioritized list of business functions and disruption scenarios that, together, will have the greatest negative impact on the business. These will serve as the basis for the next chapter – building your DR plan.

Chapter 3:

Building the DR Plan

If you've never built a DR plan, you might be thinking it's merely the steps to take to perform a recovery. While an important aspect, a DR plan is more about the business than it is about steps related to technology. The DR plan is part documentation of how things are being done today to keep the business running, and part outlining the steps that need to be taken in the event of a business disruption to see the business (and not just a given bit of technology) back up and fully operational.

The purpose of this chapter is to highlight each of the sections you should have as part of your DR plan, what should be included in each, and why.

At a high level, you should have the following in the DR plan:

Plan Goals - This section should spell out objectives of the plan such as restoring operations of critical workloads and personnel, minimizing the economic impact of the disruption, training of personnel on recovery procedures, and, if necessary, establish an alternate means of operations during a disruption.

Roles, responsibilities, and contact details – It's important to include who is on the DR Team. At a minimum, this should include any personnel involved with the building, executing, or approving of the DR plan. It should also include an organizational chart for possible use during a recovery scenario (in case it's necessary to contact, say, a department head to get input on a particular recovery issue. Contact details (phone number, work and personal email, even address) should be included here so you have the best chance of getting a hold of anyone listed in this section.

Business Function List – This section outlines the scope of data, applications, systems, and workloads the DR plan addresses. For each business function defined in the BIA (see Chapter Two for more detail), there needs to be a corresponding inventory of hardware, software, and data requirements. This will help to ensure appropriate resources – whether physical or virtual – are allocated upon recovery. Additionally, priorities established during the BIA should also be listed for each to document the order in which the systems are of importance to the organization.

Backup Procedures – Outlining backup procedures allows you to verify that the current backup strategy will help to meet the DR needs. For each backup job definition, outline the data, applications, and systems protected, tying the job back to business functions to ensure proper backup coverage. Outline the backup job frequency, type (e.g. full, incremental, etc.), which backup software is responsible (if more than one exists), and where the backup data is stored.

Recovery Requirements – When disaster strikes, there's no telling which members of the DR Team will be present or available. So, it's necessary to document all infrastructure (whether on-premises or in the cloud), software, and credentials necessary. At a minimum, a list of needs, complete with any support contact details would be prudent. Depending on your recovery model, it may be necessary to document the architecture of the recovery solution – for example, designs may assist should recovery involve failing over to cloud-based infrastructure and clients connecting remotely.

Insights: Partner-Based Review - Regardless of whether your recovery looks more like a single server or an entire data center, architecting the right environment in the cloud requires a degree of recovery expertise.

The recovery experts at CyberFortress can tailor-design a recovery environment that meets the specific needs of a given recovery, leveraging Veeam's replication technology and Veeam Availability Orchestrator to ensure the expected recovery result is achieved.

At a high level, you should have the following in the DR plan *(Continued)*:

Training Requirements – Users will need to be trained on what they need to do differently in the event of certain disruptions that alter their work environment. This part of the plan should document what training (whether proactive or reactive) is necessary, how it will be delivered, by whom, and with what materials.

Recovery Procedure – This part of the plan will likely need to be done per data/system/application/workload basis, depending on the variances in each procedure. For example, the recovering of a server image is by and large the same. But recovering a critical multi-server application to cloud-based infrastructure involves recovery of systems and data, reconfiguration of networking, and re-establishing of user connectivity. Your organization is best served by providing detailed recovery steps – remember, it may not be you performing the recovery, so this is an opportunity to pass along institutional knowledge to the person that will be handling the recovery effort.

Testing Process – There are a number of ways organizations test their DR plans. Some perform a tabletop walkthrough of the process (because of the time needed to perform an actual test). Others perform recovery simulations on a small number of critical workloads to ensure they can be recovered. And still others perform a recovery simulation of the entire environment. Whatever your choice, the process should be documented within the DR plan.

Failback Procedure – Depending on the type of disruption, failback can be as simple as restoring the recovered systems back to their original operational counterpart (as in the case of a power outage once power is restored). But failback can also be very complex – involving the rebuilding of data centers, reconfiguring how partners, clients, employees, and customers all will connect with your reinstated environment. This section should be a best effort at documenting the steps needed for – at a minimum – the more simplistic loss scenarios. For each kind of recovery scenario, define the failback steps to take to recover back to your on-premises environment, and be sure to include all necessary changes to IP addressing, DNS, and client access. Keep in mind that, should you be using the cloud as your recovery environment, you likely have the option of remaining there indefinitely, or permanently.

Insight: Making Failback Easier - While everyone knows failback is a critical part of any disaster recovery scenario, it's usually not addressed.

To simplify the process of failback, CyberFortress uses Veeam Replication. A copy of the systems in your recovery environment can be replicated back down to your on-premises infrastructure, making failback much easier. All that's needed to address is a appropriate network configuration and client access.

Because not all environments use replication, CyberFortress offers white glove assistance in seeding on-premises systems and ensuring failback is successful, no matter the scenario.

At a high level, you should have the following in the DR plan (Continued):

Update Protocol – Spell out what the process look like to update the plan, who is responsible, how often the plan should be reviewed, and some means by which to indicate when was the last time the plan was updated – usually found at the beginning on the plan.

By the time you've completed your DR plan, it will be evident whether the hardware, software, people, and processes you have in place are sufficient to meet the demands of a DR effort. In the next chapter, we'll discuss how to address any gaps in the plan that require more than you can provide today.

Blog: The 3 Most Influential People Who Help Build Your DR

Download: Business Function Inventory Table

Chapter 4:

Addressing DR Plan Gaps

Through the process of doing a business impact analysis and a risk assessment, along with building a DR plan, it's likely you're going to identify some gaps in IT's ability to meet the determined needs of the organization. Whether it's people, process, or technology, without the needed resources, recovery efforts won't be successful.

In this chapter, we'll discuss a few of the more common gaps that may be raised during the planning and offer some high-level guidance on how to address them.

Blog: Gaps In Your DR Plan

Internal Expertise - The first thing you may quickly come to realize is how little you actually know about building a plan. Sure, you know how to perform a restore of a backup, but it's likely you don't have expertise in recovering complex environments that have interdependencies at a service, system, and application-level.

The good news is building a plan involves digging into details you are already familiar with, perhaps just not in the context of planning. The challenge will be around the lack of expertise in the areas of DR planning that you don't know that you don't know. If you've never built and executed a plan, there will be caveats, one-off needs, inefficiencies, and gotchas that will rear their ugly heads at the most inopportune moment – in the middle of the recovery.

Addressing the Expertise Gap - The simple answer is you need to get someone with expertise. Only large enterprises have someone devoted (or nearly-devoted) to recovery with ample expertise. So, it's most likely that should your DR team believe you collectively don't have the necessary expertise, you'll need to engage a service provider that specializes in DR.

Staffing - The second gap you'll most likely realize exists is having enough personnel for both testing and executing and actual recovery – 61% of IT organizations don't have adequate time to perform DR testing **Error! Bookmark not defined.**, so you can imagine how much a challenge recovery will be, despite it's critical nature.

Addressing the Staffing Gap - The same DR service provider should be able to assist with your recovery efforts with anything from some extra helping hands to white-glove service.

Hardware Infrastructure - It's a given: in the case of a loss of location or infrastructure, you need equivalent-or-better hardware in order to recover. Having adequate compute, storage, bandwidth – and don't forget security – all needs to be readily available in your time of need. And most of you reading this simply don't have it.

Addressing Infrastructure Gaps - We're going to guess at this point, there are very few businesses who see purchasing a bunch of hardware that just sits there in case of emergency as a good strategy. This pretty much leave you with the cloud as the most viable option. But you have two paths you can take: The first is leverage a cloud service provider (CSP) that can offer you DRaaS, where testing and actual recovery are performed in a controlled cloud-based virtual environment that is only spun up (and, therefore costs you) when needed. The second involves proactively shifting workloads to a CSP that offers IaaS. Using this method, you proactively negate the loss of location, connectivity, system (assuming there's automatic failover at the CSP), etc.

Software - During the process of working backwards from recovery objectives to backup requirements, you may come to realize the backup software you currently use doesn't provide the level of backup frequency or methodology needed to meet your RTOs and RPOs. Additionally, you may also find that a full recovery of the environment with all its complexities requires some serious automation of the process to ensure success – and, again, your current software may not offer this.

Download: DR Plan Gap Analysis

Many of the gaps presented in this chapter require additional budget to address. This is one of the reasons we began this eBook talking about getting executive buy-in and having executive representation on the DR team. These folks will understand why the need for additional budget dedicated to DR resources is important and will an advocate for helping you get the budget allocated.

There may be other gaps you find throughout the process of developing your DR plan. In every case, there's nothing new under the sun, and each of your newly found issues have already been addressed before. So, a quick call to a trusted DR partner or even a search on the Internet will provide you with some idea of how to address the gaps.

Insights: The Need to Tailored Cloud Infrastructure

It's important to know that you can't just throw VMs up into the cloud as part of a recovery effort, or migration for that matter. Identifying the resources needed for given workloads, the placement within a virtual environment, and the resource strain that puts on the underlying physical hardware is critical so your can be sure you are able to productively operate from a cloud-based recovery environment. Similarly, some applications require physical hardware to operate efficiently.

CyberFortress offers customized infrastructure solutions – physical and virtual – to meet the specific needs of their customers. Veeam's replication capabilities can facilitate easy recovery and/or migration of on-premises workloads to your cloud infrastructure.

Insights: Leveraging Recovery Software

There are a number of technical capabilities that exist today in the world of backup and recovery that every organization should be taking advantage of. Replication should be front and center; the ability to replicate makes recovery fast and accurate. The second is orchestration of your recovery, where the entire process is scripted to ensure a consistent result.

CyberFortress uses Veeam Backup and Replication to achieve fast and reliable replicated backups of production workloads, and Veeam Availability Orchestrator to simply the most complex recovery efforts, making the process of recovery as painless and effortless as possible.

Disaster Recovery | Planning Ahead

A Practical Guide to Establishing a Proper Technology DR Plan

VEEAM Cloud & Service Provider Platinum

CyberFortress™
The Recovery People

cyberfortress.com
855-223-9322
sales@cyberfortress.com