Disaster Recovery Playbook:

The IT Playbook for Recovering Faster From Disasters

CyberFortress™
The Recovery People

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

Introduction:

The IT Playbook for Recovering Faster From Disasters

Overseeing technology isn't for the faint of heart. When systems are clicking and teams are cooking, no one will ever reach out with praise. Yet, if an outage hits, users are on top of you in seconds. Soon after, you can expect a call from the C-suite as frustrated executives watch downtime costs and complaints from angry customers accumulate.

And make no mistake, it's rough out there.

Trends

As reported in Veeam Software's Data Protection Trends Report for 2023, a survey of 4,200 global IT leaders revealed **ransomware as the most common and impactful cause of outages** for the prior three years.

Not only did 85% of respondents say their organization was successfully attacked at least once in 2022, but **nearly 40% also reported their entire production data was encrypted or destroyed** - and only 55% of it was able to be recovered.

Veeam's 2023 Ransomware Trends Report surveyed 1,200 IT leaders from organizations of all sizes and found that **ransomware strikes everyone, as do other events that can bring a company to its knees**, whether it's a fire in the datacenter or a hurricane that's taken an entire region off the grid.

CyberFortress is a global company that makes it simple to fully backup and rapidly recover all lost or stolen data to prevent damage and disruption to organizations of all sizes. We provide highly available and secure cloud data protection Disaster Recovery (DRaaS) and Backup (BaaS) solutions built on market leading technology from Veeam.

Visit protect.cyberfortress.com/data-recovery-backup

CyberFortress™ The Recovery People

Key Considerations

Regardless of the cause, unless you're prepared and poised to recover fast, it can all spell disaster. So how do you develop a winning data protection, business continuity, and disaster recovery (BCDR) strategy? You begin by looking at key considerations, namely, assessing what you have and what's at risk.

Do you have a budget for technology to close security gaps resulting from an expanded digital footprint?

Are you aware of how much downtime you and your customers can tolerate?

Have you evaluated business functions and what should be restored first?

Are there recovery point and time objectives (RPO/RTO) to meet and do you have the capabilities to achieve them?

Is your IT team sufficiently staffed and skilled to handle a complex, full recovery under pressure?

Do you know how to conduct testing and when?

These are just a few of the many critical questions to ask and the answers can expose concerning limitations. That's why many organizations enlist managed services providers (MSPs). With their cloud-based offerings, the cost and maintenance of hardware and software are eliminated. Testing can identify vulnerabilities before issues arise. Service level agreements (SLAs) can ensure RPOs and RTOs are met. And not only can MSPs help overcome IT talent shortages, their highly trained people regularly perform full recoveries and are up to speed on the latest threats.

Most importantly, MSPs help plan and implement a strong, cost-efficient DR strategy. As the Boy Scouts of America have had as their motto for more than a century: "Be prepared." When it comes to disasters and IT, no truer words have ever been spoken. It's no coincidence that we chose this as the theme for our webinar with Veeam that went through their 2023 ransomware research findings.

In the following playbook, we'll drill down on this topic, enabling you to choose the right MSP, prepare a DR plan, and ensure your company is always prepared and ready to recover faster from disasters.

IT Playbook

CyberFortress™
The Recovery People

IT Playbook #1:

Plan Your Recovery

Disaster recovery (DR) is no longer something most organizations are capable of doing on their own, and, frankly, it never really was. It's a complex operation that requires specific knowledge and experience to do well. If your organization has just experienced a massive ransomware attack or had its main data center taken out by a fire, you really don't want your DR managed by a team who's doing it for the first time. And unless your organization is very, very unlucky, that's the likely scenario if your DR is managed in-house.

So, you'll want to find a partner who can ensure that if the worst ever happens, your business can get back up and running fast. But not all service providers are created equal. You'll need to do your homework and vet your partner properly to make sure they're reliable, skilled, experienced, and up to the task.

A strong service provider will collaborate with you to design a customized DR strategy that meets your businesses' unique needs, provide options at different levels for different tiers of data, guarantee RPOs and RTOs backed by a service level agreement (SLA), and monitor the entire process end-to-end.

But just because a provider looks good on paper doesn't mean that they can actually deliver when you need them. Even if the SLA looks good, if your data center has been completely compromised by a ransomware attack and your provider takes weeks to spin up all the virtual machines (VMs) and data you need, a free month of service or a lump sum of cash won't make up for being dead in the water for that long.

Before you sign a contract, ask:

- **How long would it take to restore your entire data center at a secondary site?**
- **Have they tested that capability?**
- **Can they provide the test results?**
- **When was the last time they performed a complete failover for a customer?**
- **Can they put you in touch with customers for whom they've done a complete failover?**

Insider Tip: Ask them about the following must-have capabilities. Few providers offer even a majority of the services on the following checklist, but because they're all valuable components for your DR, you'll want as many as possible.

Your Provider Capability Checklist

- **1. Offsite VM replication:** Many DR services offer VM backup because it provides compression and deduplication to shrink the footprint of stored data. But VM backup alone will probably not be sufficient to meet RTOs for mission-critical data and systems. Instead, you'll want full VM replication — which essentially maintains an exact copy of your source VMs and can therefore enable much faster DR.

- **2. One-click failover:** Even a well-documented DR plan might require your IT team to manually implement steps and execute multiple external scripts. But if your DRaaS solution offers one-click failover, you can implement your recovery plan instantly — with a single click — whether you need it only for specific VMs or your entire site.

- **3. Hypervisor-agnostic infrastructure:** Many DRaaS providers can only help you restore data and systems across the same type of virtual infrastructure (VMware to a VMware recovery environment, Hyper-V environment to Hyper-V recovery machines). The right solution will have the ability to translate between these models and provide fast and reliable data restores across all of your virtual infrastructure platforms.

- **4. Instant file-level recovery:** What if the disaster your team is facing is simply the corruption or deletion of a single, very important file? You'll want a DRaaS system so flexible it will allow you to isolate the file in question and restore it wherever you need — whether to its original folder or a different location for faster retrieval.

- **5. Configurable WAN acceleration**: Here is a capability you'll find only with the best DRaaS providers. With configurable WAN acceleration, you'll be able to move select data to your cloud backup location up to 50x faster while using as little as 1/20 the bandwidth of a typical backup transmission. This will save your company money while protecting the operational performance of your staff's other workflow apps and bandwidth needs.

- **6. Customizable RTOs and RPOs:** When disaster strikes, restoring some data and systems — like customer credit card details and key employee workflow tools — are a priority. But you aren't likely to need archived data right away. Your DRaaS service should give you the flexibility to divide infrastructure according to urgency, so you can set RTOs and RPOs for restoring mission-critical systems right away while de-prioritizing less important items.

- **7. Flexible payment options:** Your DRaaS solution should allow you to choose a pricing structure that makes sense specifically for your business. This should include fixed pricing for dedicated computer resources, as well as pay-as-you-go costs that are based on the bandwidth you consume and can be scaled up or down anytime.
- **8. A proven third-party partner:** Keep in mind regardless of your IT team's knowledge, you very likely don't have the time or resources to manage your company's DR in-house. Even with the best DRaaS solution — Veeam's Cloud Connect Replication — you'll want the expertise of a proven third party for implementation, configuration, stress-testing, proactive monitoring, and alerts. That requires support from the most highly trained and credentialed experts in the industry.
- **9. Data tiering with different levels of cost:** Not all data is created equal and you want to determine the proper protection for different tiers. For some data and applications, you can afford to wait hours to recover. Others, however, may cripple the business if they're unavailable for more than a few minutes. Make sure you're paying for the RTOs and RPOs you require - no more, no less.
- **10. Alternate recovery targets:** In the event of a disaster, all those backups in the cloud won't help if there's no place to recover. Recovery in the cloud is definitely an option, but that's tricky given how different the architecture is from a typical data center. It's not something you want to figure out in the middle of a crisis, so if you want to go this route, it's best to leave it in the hands of experts who have already successfully architected and executed DR to the cloud.
- **11. Geo-redundancy:** It does you no good to have a backup service provider if their facility is taken out by the same forest fire, hurricane, or ice storm that took out your own. A good provider will have multiple, redundant facilities far enough away from one another so if a natural disaster strikes one, the others should be able to continue operations.
- **12. Monitoring and management:** No matter how automated the backup process may be, it still needs to be monitored and managed. Further, backups should be regularly tested for recoverability. Make sure that whatever provider you choose allows for regular and thorough testing.
- **13. Troubleshooting:** Pay careful attention to the level of service they provide. If you encounter problems after a disaster, you'll want to know you can get knowledgeable help fast to solve them.

Checklist done?
DRaaS components set up?

Test your one-click failover and failback with your provider...

Understanding DRaaS Responsibilities

In DRaaS, the provider will participate in all steps of the failover process. This includes spinning up applications and data from backups or replicas in their hosted environment, then transitioning a customer's users over to the hosted service. They will also facilitate failback, helping IT move users back to the primary environment once it's fully restored.

The customer needs to ensure the right applications and data are being protected. For example, if new VMs are added to the infrastructure, they also need to be added to the replication/backup schedule. If IT adds additional storage devices to keep up with data growth, those devices and the data inside them must be added to the schedule.

Put DRaaS to the Test

When it comes to DR, if you're not testing, it's not too much of an exaggeration to say that you're not doing DR at all. Not only do you need to ensure that every VM you spin up will work properly, but you also need to ensure that you restore in the right order. Otherwise, applications with dependencies will fail and you'll spend all your time troubleshooting instead of getting the business up and running.

Before going into specifics, here are a few general points about testing. You should test at least once a year, though ideally once a quarter. A paper test — where the team runs through the plan by talking about what they'll do around a conference table — is better than none. But ideally, you want to do a full test, even if it's only done section by section. There's no substitute for the real thing, and you don't want any surprises when you have to do it for real.

Also, remember: DR is stressful.

Customers, senior management, and colleagues are all looking to you, and if things go wrong, you're on the hook. Your team needs to be able to follow the DR plan instinctively, so they lose no time worrying whether they're doing the right thing. And the only way they can get to this point is with practice via testing.

When you do, be sure to scan all your backups thoroughly. You really don't want to restore data that's infected by the same malware that took your environment down in the first place.

Make sure you have a communications plan in place. Know exactly who is going to give status updates to whom and at what time intervals. You do not want your team constantly interrupted by scattershot queries from many different people — they need to focus fully on recovery.

Finally, after every test, make sure to update the current plan. The environment changes, and you will undoubtedly discover something new that wasn't accounted for. If you don't update the plan, you'll repeat the same mistakes when it really counts.

DRaaS Testing Environment

Practically and tactically speaking, there are a number of parts of the environment that could (or perhaps better put, should) be a part of your testing.

Let's start with the fundamental components that make up your environment:

Systems: At the core of a DR plan is the need for a given set of servers, endpoints, etc. to boot up and function correctly. You already know this one, but it's still important to at least mention it.

Directory Services: All your application servers, directory-enabled applications, users, security, and identity services rely on the directory being up and current. Testing the parts of your directory that need to be running in a disaster scenario is fundamental to the success of the rest of the recovery. This includes servers acting as Domain Controllers (DCs), FMSO role DCs, DNS, and a Certificate Authority like Federation Services (AD FS), if used.

Applications: This can be a simple application running on a single server or a complex one that leverages multiple systems and services.

Data: At this point in our industry, it feels like it's a given that data recovery will work. But testing to ensure critical data is current and without corruption should be a part of the process.

Networking: You may not have duplicate hardware, etc. at your recovery site, but applications may require specific IP addressing, access to systems or other parts of the network, external DNS rule needed/changed, and more. A simple misconfigured firewall in the recovery site can cause a critical part of the environment to not work.

Security: Many newer compliance mandates and best practices discuss the need for security to be maintained, even in the face of a disaster. Changes to security can be made at any time and, should a recovery take place, there needs to be a way to make certain these are lost in the process.

Test Considerations

Beyond components, you need to test operational elements as well. Your DRaaS provider will work with you on this and manage much of it.

Here are some considerations you'll need to address when testing:

Dependencies: There are two parts to this one. The first is simply having the application or service that is dependent upon another available when needed. As an example, having Active Directory (AD) running as part of testing your on-premises Exchange services is critical. The second part is ensuring anything involved with either side of the dependency is current. For instance, a recovered version of AD that doesn't possess a recently updated computer password for a server would keep that server from joining the domain. This could impact an application from functioning, so the server and directory recovery must be in sync.

Specific Workloads: This takes the concept of nearly every one of the fundamental components and logically combines them into one definition. Take the previous example of on-premises Exchange. The workload requires both multiple Exchange and AD servers, possibly external security-related inbound and outbound messaging platforms, and more. Thinking about workloads in this fashion will help to better define what needs to be recovered during a test.

Alternate Site: Some organizations plan to recover in the cloud. Some have varying contingency sites. Whatever the recovery location you have worked out with your DRaaS partner, it's important to not simply assume that the site is going to play well with your recovery process. Putting the site's ability to run the recovered elements of your network needs to be tested as well.

Failover: Recovery is about restoring operations, not systems and data. Practicing the actual failover of some or all of the environment – which may include firewall changes, VPN connections, IP address changes, and more – is necessary to ensure it will work when it needs to.

Employee Remote Connectivity: Recovery is useless if no one can remotely connect to it. Including a few remote employee scenarios (e.g., from home and Starbucks, using a virtual desktop or a personal one) are necessary to deem a recovery test successful.

Failback: This is less often included in DR testing, as it's the last thing on anyone's mind when you're trying to get through the disaster first. But knowing you have the ability to fail everything back is equally as important. If the plan is to, say, recover in the cloud when your on-premises environment is down, many organizations either choose to plan the failback when the disaster happens or, in some cases, just leave the environment in the cloud.

IT Playbook #2

Executing in an Emergency

If your data center is on fire, underwater, or digitally shredded thanks to a ransomware attack, it's time to put your plan into action. A strong DRaaS provider will be able to spin up applications and restore data to their cloud. During failover, Veeam Backup & Replication recovers the VM replica to the required restore point and shifts all I/O processes from the source to its replica.

So, the worst has occurred. Your data center is on fire, underwater, or digitally shredded thanks to a ransomware attack. You've notified your DRaaS partner. It's time to put your plan into action.

What's going to happen?

Recovering to a Provider's Cloud

The first thing you need to decide is where you are going to recover. If you can recover to the original equipment, that's probably best, but in many DR situations, that's not going to be possible because it's too damaged or compromised. A strong DRaaS provider will be able to spin up applications and restore data to their cloud, then fail over employee access to these resources.

During failover, Veeam Backup & Replication recovers the VM replica to the required restore point and shifts all I/O processes from the source to its replica. As a result, you have a fully functional VM within a couple of minutes, and users can access services and applications with minimum disruption.

Failovers are broken down into two types: partial and full site. In a partial site scenario, the VMs being failed over are manually selected and powered on. As an example, let's use CyberFortress failing over for a customer who is using Veeam as their DR software. Veeam Network Extension Appliances deployed in both the customer and CyberFortress environments connect to establish an L2 VPN tunnel to establish connectivity between failed over VMs and the production environment.

In full site failover, the customer and DRaaS provider will execute a pre-configured failover plan. External IPs and ports can be pre-assigned, and failover VMs will boot in a pre-specified order. No VPN tunnel is established during full site failover, but there are several ways in which connectivity to these resources can be managed, such as a replicated VPN server or VMware Cloud Director.

If it's possible to recover on-premises using failback, that may be a good option, so long as it doesn't create unacceptable downtime for the business. For a major disaster, you will almost certainly want to fail over and then fail back so that critical systems will be available during the time it takes to fail back to the primary data center. We'll cover this in the next section.

To-do list:

Avoiding mistakes that impact execution

Unfortunately, execution may not always go smoothly, especially if the customer has made one of the common mistakes below. A strong DRaaS provider will help you avoid these during planning, but the more you know ahead of time, the better prepared you will be if a complete recovery is ever needed.

- **Encryption Passwords and Other Essential Credentials:** You should definitely encrypt your backups. After all, there's a lot of valuable, sensitive information stored in them. But you need to make sure the keys are stored somewhere outside the organization such as a cloud vault or portable vault on a thumb drive. If you store them in the same environment that a disaster would destroy, your DRaaS provider will have no way to decrypt your backups. They'll be useless and you'll be completely out of luck. This advice also applies any essential credentials, such as passwords for Active Directory DSRM and essential root / hypervisor accounts.

- **Application Groups:** It's critical to know which machines have applications that communicate with others, such as a workstation that interacts with a central database. If these relationships aren't part of the plan, these apps won't function properly, if they function at all, after execution.

- **Boot Orders:** Based on application group dependencies, machines will need to be booted in a specific order. For example, single sign-on applications will need domain controllers online first before they will function.

- **DNS Time to live (TTL):** If data is accessed via a public DNS record, know whether the record has a short TTL so it can be repointed to the resource's new external IP.

- **Firewall Ports:** Understand which external NAT rules and firewall ports your DRaaS provider will need to configure for applications to function. When possible, have these pre-configured in the failover environment.

- **Communication Plans:** Make sure you have designated teams or specific people who will communicate with end-users and shareholders. Also, make sure you know how and at what frequency these communications will take place.

- **Deadlines:** A DRaaS provider will need to know if there are set deadlines and/or criteria for failing to backup locations. Make sure you have those discussions during the planning stage.

- **Cybersecurity Insurance:** Ensure you're up to speed on what your insurance policy requires in order to receive a payout after the disaster and align these with the DR plan.

IT Playbook #3

Failback to Stay Ahead

Veeam Backup & Replication has two failback methods: replica feedback and reverse seed load. Replica feedback synchronizes changes back to production and transmits data changes. Reverse seed load is a backup chain of restored workloads with a final incremental and blackout window. Veeam Instant Recovery minimizes downtime.

You've been running your business in your DRaaS provider's infrastructure long enough to have reestablished your own data center, and now it's time to failback.

Veeam Backup & Replication is a very popular DR software solution that many DRaaS providers support. If you're using Veeam, there are two primary methods for failback.

Here's what to expect.

Replica Feedback

The first is replica failback, which, if you're using Veeam Backup & Replication, is an easy, though multi-stage process. In the first stage, changes are synchronized back to production and the replica VMs are still available for end-users. This synchronization can happen with the original production VMs, one that's been restored from backups or was newly created by Veeam during failback initialization.

Next, processes are shifted from the replica VM back to production, and the replica is powered off. All data changed during the first stage is then transmitted, either automatically, at a scheduled time, or manually. You can choose the method that will best allow your organization to perform failback during a window of time that works for the business and ensures application consistency.

Finally, failback is committed and operations remain in production, or failback is reverted and workloads transition back to the replica. This needs to happen as soon as replicas are powered off and the transfer of data changes is complete.

Reverse Seed Load

The second method is called reverse seed load, and it's most commonly used for workloads protected exclusively by Veeam Cloud Connect backup. It can also be used in situations where replica VMs are very large and customer bandwidth is too small to enable a responsible transmission time for replica failback. In this method, a backup chain of restored workloads is sent to the customer site using the Cloud Connect protocol or a seed device.

Once the data has arrived on-premises, a final incremental is transmitted to incorporate all changes made during transit. A blackout window is also opened where the restored workloads are powered off to freeze changes before restores take place in the production environment. These restores typically utilize Veeam Instant Recovery where possible to minimize downtime during the process. Alternatively, per-VM blackout windows can be used with additional incremental backups to perform full VM or bare metal restores one at a time.

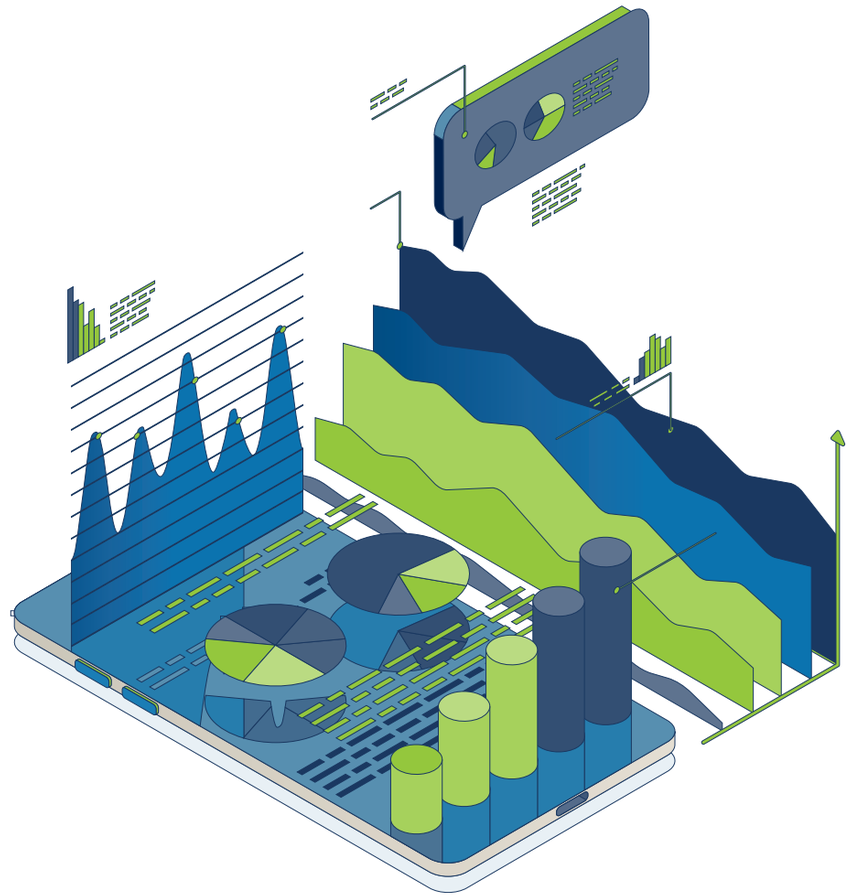
If neither of these options is feasible, it is possible to physically ship applications and data pre-loaded onto physical media. This is an expensive option, but in cases where there is a very large amount of data that needs to be transferred, this may be the fastest way to move it back to the company's data center. Additionally, to keep data continuity during the blackout window, Veeam Cloud Connect would still typically be used to transmit any changes that occur within the shipping time period.

IT Playbook #4

Documentation and Analytics

After successfully recovering from a disaster, it is important to document the process and analyze it for opportunities to improve. This includes understanding the root causes of the disaster and identifying measures to prevent it from happening again. Conduct a thorough assessment of the DR plan and execution, noting each issue and how they can be addressed.

Make sure that everything learned from the analysis informs the updated plan. Leverage CyberFortress' Four-Step Backup™ process executed by their Rapid Recovery Force™ to help clients recover from disasters.



Mitigate Risk

You've successfully failed back and the business is working as normal again - but you're still not done. There's one more step and that's to document how the DR process went and analyze it to find opportunities to improve. Hopefully, there won't be a "next time," but if there is, you don't want to repeat any mistakes — you want it to go even more smoothly. This is more than just a post-mortem. It's an extension of the continuous improvement that should be occurring during regular testing and ongoing planning.

First, attain a deep understanding of the root causes of the disaster. If it was a fire, what caused the fire? What fire suppression methods were attempted and why did they not prevent the disaster? In the case of ransomware, determine what type of malware was used, the vector that cyber criminals took to implant it in the environment, the systems it compromised, and how long it was present within the network before it began encrypting data.

Whatever the disaster, once you understand how it happened, identify measures the organization can take to prevent it from taking place again. Look to mitigate risk and contain the damage it may do in the future. Throughout the entire process of the initial disaster, recovery, and failback, make sure the team takes notes on what was done and how it worked.

DR Plan Assessment

Next, conduct a thorough assessment of how well the DR plan and execution worked. Was the team able to meet its RPOs and RTOs? Were there issues that stalled recovery? Did applications boot in the proper order so they could function? Step by step, identify how well the plan matched what actually needed to occur and how well the team executed the plan, noting each issue and how they can be addressed. In cases where those issues cannot be reliably prevented from occurring again, document them with symptoms and resolution steps so that your team can more quickly resolve them in the future.

Most important: make sure that everything learned from the analysis informs the updated plan. Take action. Don't just let the analysis linger in a file somewhere, untouched and unused until the next disaster occurs.

At CyberFortress, we ensure that our clients are able to recover from any disasters thanks to our Rapid Recovery Force and our Four-Step Backup™ process. Our Rapid Recovery Force™ provides our clients with a 24/7 recovery hotline where callers are guaranteed to speak with a human CyberFortress employee to address their problem. Our specialists are certified experts in the technologies we use, and our team works exclusively on customer recovery 24 hours a day, 365 days a year.

CyberFortress Four Step Backup Process:

Complete data map and inventory: We find and locate all of a client's data.

Custom data recovery plan: Our team will develop a customized plan to ensure our client can recover in time to avoid damage to the business.

The Fortress to secure client data: Backup data is protected in a secure, geo-redundant facility.

Continuous readiness reporting: Our clients never wonder whether their data can be recovered. We keep clients updated with regular reports on recovery readiness.

Questions about findings can be sent to **sales@cyberfortress.com**

With CyberFortress as a partner, we help organizations build a DR plan that works, backed by professionals who have performed dozens of full restores throughout their career, so clients can be sure that the plan will be executed flawlessly.

When disaster strikes, you want a DR plan and a DR team that will get you back in business fast. That's exactly what we do for our clients, every day of the year.

Disaster Recovery Playbook:

The IT Playbook for Recovering Faster From Disasters

CyberFortress™
The Recovery People

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