Why Modern IT Requires Modern Disaster Recovery

Dan Keldsen, Alan R. Earls, Ed Tittel, James Green

INSIDE THE GUIDE:

• Why Legacy Disaster Recovery Can’t Keep Up Anymore
• How To Respond to New Threats Like Ransomware
• Disaster Recovery as a Service: a Better Way
Why Modern IT Requires Modern Disaster Recovery

AUTHORS
Dan Keldsen, Alan Earls, Ed Tittel, James Green

EDITOR
Keith Ward, ActualTech Media

LAYOUT AND DESIGN
Olivia Thomson, ActualTech Media

Copyright © 2020 by ActualTech Media

All rights reserved. This book or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of the publisher except for the use of brief quotations in a book review. Printed in the United States of America.

ACTUALTECH MEDIA
6650 Rivers Ave Ste 105 #22489
North Charleston, SC 29406-4829
www.actualtechmedia.com
Introduction: Welcome to the Future .............................................. 7

Chapter 1: Welcome to the Future .............................................. 7

Chapter 2: Why Is Disaster Recovery So Hard? ......................... 8
  The Scope of Disasters ................................................................. 9
  What Makes It Hard to Do DR Well? ............................................ 9
  The 3 Challenges of Legacy DR: Expensive, Complex, Unreliable ................................................................. 10
  Compliance Checking—the Elephant in the Room .................. 12
  The Devil's in the Threat Details .................................................. 12
  Old-School Threats ................................................................. 14
  Modern Solutions = Disaster Recovery Excellence .................. 15
  Your DR Future = Public Cloud, Orchestration, and SaaS ....... 16
  Disaster Recovery Can Be Hard: But Must It Be? ...................... 18

Chapter 3: Backup Does Not Equal DR ....................................... 20
  Disaster Recovery Defined ............................................................. 20
  Exposing Inadequacies ............................................................. 22
  Putting Backup in Perspective ..................................................... 26

Chapter 4: Stone Age vs. Space Age DR ................................. 27
  Stone Age Approaches .............................................................. 27
  Reaching for the Stars .............................................................. 30
  Adopt Space Age DR or Face Extinction ................................. 33

Chapter 5: 5 Ways to Do DR Better .......................................... 34
  Rethinking DR for the Future ..................................................... 34
1. Don’t Build a DR Site at All .................................................................35
2. Make Your IT Budget Go Farther and Do More.................................37
3. Gracefully Sidestep Ransomware......................................................38
4. Backups Are Ineffective; Focus on Recovery.................................42
5. Have Faith in Your DR Plan.................................................................44
Do Disaster Recovery Better.................................................................48
Survival of the Modern..................................................................49
The Gorilla is the professorial sort that enjoys helping people learn. In the School House callout, you’ll gain insight into topics that may be outside the main subject but are still important.

This is a special place where you can learn a bit more about ancillary topics presented in the book.

When we have a great thought, we express them through a series of grunts in the Bright Idea section.

Takes you into the deep, dark depths of a particular topic.

Discusses items of strategic interest to business leaders.
ICONS USED IN THIS BOOK

**DEFINITION**
Defines a word, phrase, or concept.

**KNOWLEDGE CHECK**
Tests your knowledge of what you’ve read.

**PAY ATTENTION**
We want to make sure you see this!

**GPS**
We’ll help you navigate your knowledge to the right place.

**WATCH OUT!**
Make sure you read this so you don’t make a critical error!
Welcome to the Future

Welcome to this Gorilla Guide To...® Why Modern IT Requires Modern Disaster Recovery. If you’re looking for ways to protect your environment from the many threats it faces today, you’ve come to the right place.

This goal of this book is to take a close look at backup and disaster recovery in the modern age of computing. To do that, we also need to examine where we came from; how we got here; and where we go from here, as it relates to backing up and then restoring your critical systems and data.

When you’re finished with this Gorilla Guide, you’ll have a strong grasp of the challenges facing organizations today when it comes to protecting their infrastructure, as well as a good understanding of how to meet those challenges. It’s a complicated topic, to be sure. That’s why this book exists.

No one wants to have a disaster hit their data center, of course—but the reality is that it happens. And it’s happening more often than ever, with the rise of new threats from the outside. That means new ways of responding are necessary. We’ll show you some of those new methods.

So let’s get started. We begin with a question you’ve undoubtedly asked yourself, probably many times.
CHAPTER 1

Why Is Disaster Recovery So Hard?

In the 21st Century, we’ve come to expect that technology will simply work, all the time, night or day, on a mountaintop, in the air, in our cars ... everywhere. Always.

In fact, it’s not just whether a service or application you want to use is up or down—raw performance matters, as well. Did you know that every 100 milliseconds of delay when loading a website will send consumers to competitor sites, at an estimated conversion rate impact of up to seven percent to the business?¹

Imagine the impact of being down for several hours, or, worse, days.

And yet while technology has become more reliable, more consumer-friendly, and ever better, faster, and cheaper, there’s a reality we must all acknowledge:

No matter how good your infrastructure is, you’ll have to deal with various types of disaster—it’s simply a matter of time, and the latest statistics indicate you’re more likely than ever before to experience a disaster.

The Scope of Disasters

IDC estimates the average cost of downtime at $250,000 USD per hour across all industries and organization sizes. For a total downtime of only eight hours per year, the average cost would be $2 million USD.²

Combine that with IDC’s estimate that “as many as 50% of organizations could not survive a disaster event,” and the ramifications for poor disaster recovery (DR) come sharply into focus.

Welcome to the world of DR: The decidedly unsexy, often-ignored safety net of your business. Done badly, however, it threatens the heart of your business—the results you deliver to your customers, partners, and employees.

Like all technology trends, DR is in a race to keep pace with other innovations in technology and continuously high customer/user expectations. And in a world of regulatory scrutiny, cybercrimes like extortion with ransomware, power outages, and natural disasters, operating a business without functioning DR is like playing Russian roulette with the fate of your organization, or driving a vehicle with no training and no insurance.

Luck is not a viable strategy, and DR is no place to skimp on strategy, tactics, and thoroughly tested execution. And while some may claim that DR has evolved slower than other IT fields, there are signs that desperately needed innovations have finally caught up with the more exciting aspects of tech.

What Makes It Hard to Do DR Well?

Here’s the challenge: The traditional point of view on DR was focused on recovering from natural disasters. These disasters were relatively rare, and predictable as far as what type of natural disaster might hit any given geography.

² Source: IDC August 2019 Whitepaper “The State of IT Resilience”
But they did happen, and when they did, getting systems up and running again was often a nightmare. And that was in the olden days—the “complex integrated systems” of yesterday were nowhere near as complicated to understand and restore as today’s distributed frameworks of networks, storage, applications, and so on.

The simple truth is that yesterday’s DR solutions simply aren’t up to the complexity of today’s modern-day systems and the threats we all face.

The 3 Challenges of Legacy DR: Expensive, Complex, Unreliable

Traditional DR implementations have fallen behind as new investments in technology implementations within organizations have been targeted more directly at customer- and consumer-facing systems.

There are three primary weaknesses of legacy DR solutions as compared to modern DR offerings, as you can see in Figure 1.

1. **Expensive:** Redundancy is normally good for DR, but it’s bad for your budget and sanity. Why? Legacy DR can require as many as five different products to manage your data twice—for both your primary site and your DR site. The typical DR toolkit includes primary storage management, backup, DR tools, and encryption tools—all handled by different solutions. This is both expensive
and fragile, as these cobbled-together solutions were never meant to work together in an orchestrated and cohesive fashion, leaving gaps to be filled with manual processes.

2. **Complex:** Runbooks that are managed across multiple tools in the traditional DR toolkit are exceedingly complex to coordinate. Extensive documentation for related personnel must be created as a companion guide to fill in the gaps where automated runbooks leave holes in your ability to recover.

3. **Unreliable:** As soon as anything in your data center changes, your runbooks and documentation are out of date. That can completely invalidate your DR plan, putting your entire infrastructure at risk. Your DR team has to carefully adjust, test, and verify all over again—and brace for the next set of changes that puts you back on the “lather, rinse, repeat” treadmill. Not good.

### Too Many Parts to Handle Manually

Beyond the problems of legacy DR, reliable, large-scale DR is hard because it touches every component in the data center, including app servers, file servers, hypervisors, networking, primary storage, backup storage, and any extension into cloud resources. It’s hardly an exaggeration to say that planning, testing, and successfully executing a DR plan and surviving the experience is one of the most difficult feats to accomplish in ITOps.

Just as automation and orchestration have opened an entirely new world of capabilities for developers through the practice and technologies behind DevOps, the only sane path to future-proof DR is to apply similar techniques and rigor to DR.
Compliance Checking—the Elephant in the Room

The million-dollar question for any DR plan is: “Will it actually work when we need it to?”

The only way to know is to test, and yet testing a DR plan can be as heart-stopping as an actual DR event. Given how complicated most production environments are, it’s extremely likely that changes will be made in the environment that the DR team doesn’t know about, invalidating the “known good” status of the runbook.

The single best way to handle that challenge is to move to a “trust no one” approach that continuously validates that the runbook is accurate and workable.

This can be done by checking foundational elements such as working network connectivity between your primary and DR sites; ensuring that file shares are up and available; and a variety of other “environment readiness” checks that ensure the runbook can safely execute.

In the past, these kinds of compliance checks were performed *maybe* as often as once a month—although more typically, it happened quarterly or even yearly. But in a world of automation everywhere and constant change, it makes more sense to continuously check. Modern DR, with its automated compliance checking that both validates and indicates exactly what has fallen out of compliance, is a lifesaver.

The Devil’s in the Threat Details

Consider the complexity of the systems underpinning your organization’s ability to operate with these rising threats:

- Ransomware
- Power outages
- Natural disasters
• Human error
• Hardware failure

That combination has made the threat landscape dramatically larger than it’s ever been. Take ransomware as the scariest new example. According to recent research, it’s the No. 1 cause of DR events (Figure 2).

Sometimes these attacks are specifically targeted at individual organizations, and you may feel that your organization isn’t on the radar of a potential attacker. That would be an extremely unwise position to adopt.

Whether it’s research from well-known analyst firms, or “in the trenches” security firms, all the statistics indicate that ransomware operates at a truly massive scale:

• Gartner Inc. reports a 700% increase in ransomware since 2016.
• Fortinet estimated the cost of ransomware in 2019 would be $11.5 billion.

**Figure 2:** According to the report, “The State of Enterprise Data Resiliency and Disaster Recover 2019,” ransomware is the No. 1 cause of DR events.
• Sophos says that 75% of companies infected with ransomware thought they were thoroughly protected.

What’s the average cost to recover from a ransomware attack? According to research by Kaspersky Lab, ransomware costs an average of $713,000 per incident when factoring the cost of downtime and lost business due to reputational harm.

If you choose to pay the ransom, ransomware payouts range from thousands to millions of dollars to get your data and systems back. Like most forms of blackmail, if you pay, there’s no guarantee that everything will be intact or that you won’t be targeted again. And this is exactly why you need to make sure you’re shifting from a reactive strategy for DR to a proactive strategy that protects you against these sorts of threats.

**Old-School Threats**

Traditionally, the threats that IT teams worried about revolved around power outages, natural disasters, and hardware failure. These remain real threats, too, and they have also increased over time.

It’s no secret that electrical grids are often stretched to capacity, and that wildfires, floods, blizzards, and other natural disasters can take down powerlines and network connectivity.

For a recent example, look no further than the combination of droughts and extreme power usage in California in 2019. Large sections of the state were shut off from the grid for as many as seven days. If your DR plan for power outages only allows for 24 hours of emergency power, what’s your fallback plan when something like this happens?

**Human Error**

Human error is an overlooked and unsexy reason that DR plans need to be enacted. It doesn’t take a natural disaster to bring a business to its knees—without the proper controls, an admin can click the wrong
button and take the entire infrastructure down. It’s an entirely inno-
cent mistake, but that won’t matter to the C-level execs when they’re
looking for someone to blame for the mess.

It may not even be the admin’s fault, given the huge complexity of DR. As much as we’ve learned about great user experience for consumers, those lessons haven’t necessarily trickled down to sys admins and ITOps—things should be simple and easy to use for them as well.

“All these reasons make it clear that you can’t simply hope for the best when disaster strikes. An organization must be prepared, and the dirty secret of DR is that most plans have never truly been stress-tested to confirm that when disaster strikes, the plan will restore normal oper-
ations at all, let alone within a reasonable time frame.

And failing back to your primary data center? This is even more rarely tested, and often much more difficult than expected.

Modern Solutions = Disaster Recovery Excellence

DR isn’t new, but like many tech investments in security or areas that cost money instead of making it, DR capabilities are often woefully in-
sufficient to meet the needs of an organization to successfully weather an incident.

Many technology implementations lag the leading edge of technology, with new implementations replacing technology that’s often two to three generations behind the cutting edge.

“The Field Guide to Understanding ‘Human Error’”
by Sidney Dekker has extensive examples from a variety of industries on the psychology behind human error, both from a design and user perspective.
If your existing backup and DR solutions are five to seven years old, it’s worth looking at more modern approaches, as a lot has changed in that time. One of the biggest changes, as noted by IDC, is that organizations are tired of the inefficiencies and expense of silos:

*Backup and disaster recovery solutions are consolidating into a single-solution platform. Over 90% of respondents said that, over the next two years, they are likely to pursue a convergence of backup and DR tools while eliminating redundant tools. This indicates that users increasingly see backup and DR functions as complementary assets of a single solution—not as separate, siloed products.*  

—Source: IDC August 2019 Whitepaper “The State of IT Resilience”

And while backing up to the public cloud continues to be a rising phenomenon, the challenges of using public cloud resources as a secondary data center for DR purposes have been difficult to overcome with legacy backup approaches.

**Your DR Future = Public Cloud, Orchestration, and SaaS**

Unfortunately, that legacy continues its stubborn hold on many organizations. As much as public cloud and software as a service (SaaS) models seem to be everywhere, they’re just now becoming mainstream for companies that didn’t start their business in the cloud.

According to 2019 research from Gartner, “in 2022 in the [United States], 14% of total IT spending will be on cloud services.”

Combine that with the continuing trend of company-owned data centers being shut down, and the shift to the cloud is quite clear: “Gartner predicts that by 2025, 80% of enterprises will shut down their

---

Top Disaster Recovery Headaches

Many organizations still struggle with the cost, complexity, and orchestration of their data protection and DR solutions. 45% of organizations indicated challenges with restore reliability, while 44% indicated challenges with backup reliability. Complexity was also a leading challenge for 43% of organizations.

—Source: IDC August 2019 Whitepaper “The State of IT Resilience”

traditional data centers. In fact, 10% of organizations already have.⁴ [Editor’s note: 10% as of Aug. 5, 2019, reporting.]

Just as organizations struggle to keep multiple environments available and current for development purposes, often with test, QA, staging, and production environments, the readiness and suitability of a second entire data center that’s ready to leap into action is historically difficult and expensive to maintain.

That’s why, if you haven’t already made a shift to the cloud, using DR in the cloud will get you moving in a modern direction, while also removing significant risk.

The raw cost avoidance of owning and operating an entire second data center in favor of on-demand resources will free up budget that you could put toward other high-visibility and revenue-impacting projects such as artificial intelligence, machine learning, big data, and personalization.

⁴ Source: “The Data Center Is (Almost) Dead” (https://www.gartner.com/smarterwithgartner/the-data-center-is-almost-dead/)
The evolutionary curve for backup and DR is clear—and if your DR solution can’t recover in minutes to hours, at a price point that leaves your funds clear for value-producing activities, it’s time to revisit your plans (Figure 3).

**Disaster Recovery Can Be Hard: But Must It Be?**

As you’ve seen, DR is complicated: Almost every bit of your infrastructure is involved. That includes storage, both primary and secondary; networking; physical and virtual servers; applications; and more. That’s a lot of moving parts. But does that mean it has to be hard?

Not at all! The complexity of doing DR right won’t go away. However, there are new ways to handle this loathsome chore. For instance, having a trusted solution means you and your staff will be freed up to pursue more innovative work, including more proactive initiatives that can boost your bottom line. Additionally, consider:

- Using on-demand, cloud-based DR resources like VMware Cloud on AWS to replace the burden of operating a dedicated DR site

**Figure 3:** Backup and disaster recovery are ready for the next transformation
• Adopting a SaaS-based DR orchestration that gives you failproof and pushbutton failover capability you can count on

Next up, we’ll probe deeper into the distinctions between backup and DR, and dive into some fundamental concepts.
CHAPTER 2

Backup Does Not Equal DR

For decades, backup was the only thing you needed to worry about if you were a data administrator or IT director. Everyone did it, often through highly manual processes. The advent of cloud-based backup was a step in the right direction, but in practice, did not fully meet the needs of most organizations. With the growth of new information technologies and the changing nature of IT operations, it’s becoming clear that more modern approaches to backup and recovery are needed to address modern challenges.

In fact, though many organizations still rely on purpose-built backup systems, these systems are really insufficient for the massive recovery needs of organizations operating in the 2020s, and certainly can’t fulfill the requirement for faster Recovery Time Objectives (RTOs) to keep pace with the demands of business. They do little but create organizational stress, and at best deliver sub-standard results.

The evolution toward a more holistic approach to backup—that is, business continuity/disaster recovery (BCDR)—signals that the inadequacy of backup for modern needs is finally being recognized.

Disaster Recovery Defined

In contrast with backup, disaster recovery (DR) is primarily focused on recovering critical data and is, arguably, a subset of business continuity, which focuses on avoiding disruptions of any kind in business operations. DR plans usually seek to identify mission-critical functions and data for which the RTOs and Recovery Point Objectives (RPOs) are
The Backup Plan ‘Sniff Test’

If your backup plan can’t answer these questions, it fails the test: Can they really deliver and meet RTOs and RPOs? Have they been tested regularly to ensure they really work? And what about compliance?

Beyond the simple requirement to provide data retention and protection required by various compliance mandates, there are also availability expectations.

A backup plan (and its actual delivery) must continue to protect data throughout the process, no matter what needs to be restored. Furthermore, that restoration must generally be fast.

devised (see Figure 4). As such, it’s built directly on the process of backup and depends on the quality of that toolset for its effectiveness.

To be effective, your backup plan should include provisions for encrypting data, both in transit and at rest. Depending on the damage done that triggered the need for recovery, the recovery process could force an organization to reacquire and reload application software, adding considerable time and cost.

Backup and DR isn’t quite as difficult as it was in the days of tape. Modern disk and solid-state drive (SSD) storage are much faster in terms of moving data, potentially making recovery easier. However, IT departments have learned the hard way that restoring physical and even virtual servers across backup sites is a very time-consuming process that can require reinstallation of operating systems and other applications, and perhaps reconfiguration and tuning before everything is again “just right.” Falling far short of the “promise” of backup and any hoped-for ability to recover from a disaster, the process often takes days and even weeks.
Exposing Inadequacies

Some companies have tried to leverage the lower cost and inherent flexibility of the public cloud to support their backup needs—and vendors have also leveraged the same technology. But this turns out to be at best a half-measure, only nominally less cumbersome than maintaining a backup site or spare machines.

And it comes with problems of its own. For instance, just as with moving any on-premises function to the cloud, a degree of refactoring may be necessary. Sometimes, in effect, the whole backup set must be “translated” into a cloud-compatible instantiation. If this were merely a migration activity, not to be repeated for months or years, that might not be a problem. But when the intent is to return all that data to an on-premises facility or even another cloud, there’s a substantial need to once again refactor—which, at a minimum, requires time and expense and could potentially introduce errors.

So, particularly if your RTO requirements are measured in minutes, traditional approaches to backup are simply inadequate. Think about...
the fact that it can take days to rehydrate data from Amazon S3 storage, for instance.

Furthermore, even with the efforts that have been made to overcome these challenges through cloud-based approaches, most existing solutions come with budget-breaking costs to cover licenses, consulting, or dedicated resources. Additionally, they’re not easily tested, and often require abundant staff, skilled in DR management. This is why standalone backup tools are starting to disappear—organizations are realizing that converged backup and DR is the future.

Backup is about protecting data, and until recently, the main focus has been on factors like human error, natural disasters, power failures, or serious hardware malfunctions.

But it’s a new era. Damage to the logic and data of systems through external attacks—especially ransomware—has become one of the top triggers for a backup recovery process. This often means the same people in an IT organization who are putting out the breach-related fires and watching for new assaults are also supervising backup and recovery processes. That’s a formula for failure, because even the most talented and dedicated teams will begin to fail under the stress—potentially multiplying the damage and disruption of the attack.

That’s why an organization also needs to think about recovery, validation, and DR orchestration—helping reassemble the components of a backup and bring back functionality. Remember: backup systems are built for just that—backup. They’re not built for, nor meant for, recovery. As many companies have found out through the years, backups fail you at the exact moment that you most need them.

**Backup Fundamentals: Data Recovery**

Organizations are forced to recover data for many different reasons. It’s still quite common for someone to simply make a mistake. An end user could inadvertently delete critical information. A disgruntled employee might deliberately harm a system. Power can fail. Or, an
external actor could commit an act of cyber vandalism or seek to profit by seizing or controlling data, as with ransomware. That’s why organizations usually work hard to create backup and restore capabilities.

Backup is foundational, but actual data recovery is what can spell the difference between going to work on Monday or looking for your next job. Without well-thought-out, well-designed, and capable recovery, it’s like putting your life savings in a safe and then misplacing the combination.

For many organizations, the recovery process is fraught with duplicative functionality and multiple vendors that are all supposed to work together in every imaginable scenario. The nature of the data loss often dictates the recovery method; with multiple systems used for various types of recovery, the system is fraught with complexity.

Usually the recovery plan focuses on providing rapid access to a modest set of the most critical information. Much effort goes into the process of determining what to recover first, and then setting RTO/RPO targets for other data or functions that are presumed to be less critical.

**Backup Fundamentals: Validation**

None of that process will matter, however, if your backups are no good. It’s mystifying, then, that validation is an often-ignored aspect of recovery. Like the old adage, garbage in equals garbage out—unless it can be verified that the correct data has been recovered, there’s a possibility that a disaster can actually expand in its consequences. Mechanisms for countering this vary in effectiveness and efficiency, but are an essential element of validation.

**Backup Fundamentals: DR Orchestration**

Recovery is always comparatively easy on paper. Plans for how things should work can seem convincingly thorough, but actual incidents that cause a DR process to go into effect happen at inconvenient times or in more complex ways than ever anticipated. Maybe the right people aren’t available, or perhaps a setting or configuration error or a planned
maintenance event made an important resource unavailable. Suddenly, those RPOs and RTOs seem far less obtainable.

While most organizations still define certain data or applications as being mission-critical, a more realistic assessment would likely reveal that most or all applications and data are, in fact, mission critical. Much of this is a matter of interdependencies between and among applications and the data on which they rely. This can extend to scores or even hundreds of different functions across the physical and virtual infrastructure and the cloud.

Bringing all that functionality back isn’t a simple plug-and-play action. For instance, some applications depend on data or functionality in other applications in order to come back to life. These dependencies are often not obvious and are seldom fully documented. So, while it might be possible to quickly regain access to data deemed critical, whether this will be enough to even start a full recovery process is less than certain.

**Figure 5:** Disaster recovery needs a complete makeover—there’s too much happening, in too many places, for manual effort to properly get the job done.
Adding to those challenges is the fact that DR, since it involves so many facets of the data center, and hundreds or even thousands of steps, is too complex to be done manually anymore. Figure 5 shows some of the factors that have to be considered.

Only more modern approaches that incorporate automation and orchestration have a hope of reliably achieving the RPO/RTO goals that are central to most organizations.

Putting Backup in Perspective

Understanding that backup doesn’t equal DR is a step toward mastering data protection challenges. It’s no longer a simple challenge with simplistic solutions from times past. DR, in a modern context, is about how fast and how non-disruptively you can recover from a disaster. It means recognizing the real needs of an organization and making a commitment to acquire the tools and techniques needed for the 2020s.

That means leveraging the full benefits of the cloud, and considering disaster recovery as a service as a potential solution to these issues. That’s what we turn to in Chapter 3.
The goal for DR, as spelled out in Chapter 2, is to get things working again (if not on the original IT infrastructure, then on a reasonable replacement). Until that happens, an alternate IT infrastructure that operates elsewhere—in another physical location or somewhere in the cloud—must serve the needs of customers, staff, and partners.

Traditional DR—the “Stone Age”—is a complex, cumbersome, and often expensive set of processes, procedures, and technology choices that usually relies on access to an alternate physical location with power, equipment, and connectivity to stand in for the normal IT infrastructure.

Modern DR—the “Space Age”—involves an agile, virtualized set of cloud-based technology choices. A cloud service provider supplies the underlying infrastructure. In addition, a rich and robust set of software-defined capabilities sets up and enables a cloud-based, virtualized replica of the infrastructure.

Stone Age Approaches

Traditional DR regimes belong to the discipline of “incident management.” This means someone with sufficient authority, designated in advance, declares when a disaster occurs. That declaration spurs the mechanics of recovery into motion. A key first step is to put a DR team—also designated in advance—to work. This team takes responsibility for implementing a carefully mapped-out DR plan, with specific recovery goals, objectives, and milestones.
While the outage continues, the team remains responsible for implementing the plan and providing a working, alternative IT infrastructure. The switchover process from normal to recovery operations is called *failover*; switching back from recovery to normal operations is called *failback*. Traditional DR usually centers on an alternate physical site for IT operations, which can be in three modes:

- **Hot.** Ready to take over in minutes
- **Warm.** Ready to take over in hours
- **Cold.** Ready to take over in days to weeks

Thus, traditional DR is based on process as much as technology. It functions mostly as a human-driven activity, with replacement systems called into service as they become available. When automation is used in traditional DR, it’s limited in scope, functionality, and flexibility. Also, traditional DR requires extensive planning, maintenance, and hands-on effort to set it up and keep it working. Each such implementation is custom built—a one-off design to match a specific IT infrastructure.

---

**Is legacy disaster recovery too complicated, expensive, and hopelessly outdated?** If you ask almost any enterprise IT admin, the answer is a big Yes!

Steve Duplessie, founder and senior analyst at Enterprise Strategy Group, may have said it best: “Let’s face it—DR has been more disaster than recovery. It has been virtually impossible to have legitimate DR for decades, and the problem just keeps getting worse with exponential data growth and overall complexity.”
Keeping traditional DR current and working means regular practice events are scheduled, undertaken, and analyzed afterward. Manual efforts keep the DR plan in sync with actual experiences and problems, and changing conditions. This is a huge issue for traditional DR, which can encounter significant difficulties with scaling and moving into and out of the cloud, especially during failover and failback phases.

Another type of traditional DR is a kind of “white glove” service from managed service providers (MSPs). Usually, that means an MSP arrives onsite and works with the local IT team to pull together its take on traditional DR.

Invariably, legacy DR incorporates multiple point solutions from favored vendors for backup, storage, failover/failback, and more. It becomes an unwieldy combination of too many pieces and parts, making it unacceptably complex and fragile.

**Disappearing Disaster Recovery MSPs**

Whether traditional DR comes from in-house resources or relies on an MSP, it uses a legacy approach that relies on brute force and big financial outlays to get recovery done. In fact, traditional DR doesn’t take advantage of intrinsic cloud capabilities, even when cloud-based compute, storage, or connectivity is part of the recovery process.

The old-fashioned, physical instantiation needed for traditional DR isn’t proving to be good business, either. Traditional MSPs are struggling to redefine themselves as cloud service providers (including some disaster recovery as a service [DRaaS] offerings), with varying degrees of success. Gartner comments on the need to check provider financial strength and viability in its latest Magic Quadrant for Disaster Recovery as a Service.5

---

In fact, Gartner no longer covers traditional DR with a Magic Quadrant. Further proof of this shift is found in the fact that 2019 witnessed numerous high-profile MSP bankruptcy actions, including big names like Sungard, Fusion Connect, Cryptopia, and Bridgehead Networks, among others.

Another sobering truth is that developers aren’t building on-premises applications anymore. Thus, service providers of all stripes—including MSPs who may or may not be cloud-savvy—all offer cloud-based implementations. This is perhaps a blessing in disguise, because traditional DR involves what can only be called “tool and infrastructure sprawl.”

This means some organizations find themselves stitching together components in a DR patchwork. Those components often include primary and backup data centers, backup solutions, DR, encryption, and virtualized cloud services. They may involve as many as half a dozen vendors or service providers to do all this.

Reaching for the Stars

Modern DR makes good on a spectacular proposition. It offers the ability to make your data instantly and inexpensively available in the cloud. How is this possible? It leverages the cloud in two important ways.

First, it uses cloud-based storage for backup that is both cheap and deep (that is, inexpensive and inexhaustible). This means that during normal operations, cloud storage serves as a convenient and durable backup receptacle.

Second, it uses the power to create compute on demand when a disaster occurs. The cloud’s “pay-as-you-go” model means that unless and until disaster occurs, organizations need not pay to duplicate data centers or infrastructures just in case they might need them sometime. The meter only starts running when a disaster is declared, and an alternate instance of the IT infrastructure is needed ASAP.
The cloud has another significant advantage, one that often flies under the radar: the ability to have runbooks in the cloud that can automate the stitching together of all components needed for DR. This provides true one-click failover.

Modern DR is also quite nimble. It’s based on backup into the cloud, and serves as part of a more general, overall digital transformation process for many organizations. Modern DR is available in a variety of cost models, allowing companies to balance RTO and RPO intervals against the costs involved. You can choose to spend more, and failover more quickly; or spend less, and failover more slowly. The point is that the choice is yours.

Modern DR is also flexible: You can set it up one way this week and another way next week, thanks to its virtualized, on-demand, software-based definition and use of powerful automation tools.

This is radically different from traditional DR, where you can spend half a year building out a secondary data center (and once built, its assets remain on the books until they’re fully depreciated). Modern DR can turn...
on a dime, and easily be reconfigured to add new elements, remove old ones, target different storage, set up new virtual data centers, and more.

The mobility that’s inherent to modern DR lets organizations tackle both planned and unplanned outages. Thus, modern DR tools are useful for workload migration (which may go into the cloud or to another data center) and data center modernization, in addition to standing ready to take over should an actual disaster occur.

Because modern DR includes built-in data integrity checks and end-to-end encryption, it offers improved security. Similarly, it allows tests of recovery operations to occur anytime, but doesn’t impact normal IT operations.

This means organizations can test DR whenever they like, using the same push-button DR capability for testing they’d employ in an actual disaster. Datrium DRaaS, as Figure 6 shows, puts all the pieces together under a single technology umbrella, all under the control of a single, centralized orchestration and automation facility.

Figure 6: The modern approach treats disaster recovery as a service (DRaaS), which brings backup, DR, and cloud recovery under a single technology umbrella.
Adopt Space Age DR or Face Extinction

In sharp contrast to traditional DR, modern DR is a simple proposition. It lets buyers choose appropriate RPO and RTO targets. Modern DR uses cloud-based solutions that combine backup and DR capability directly and seamlessly.

Based on demand-driven DRaaS, modern DR lets organizations shift DR capital expenditures (CapEx) almost entirely over to service-based operational expenses (OpEx). This lets them forgo capital allocation, depreciation and amortization, along with physical asset management and provisioning. It adds up to a lot less worry.

Using modern DR, organizations can also manage and monitor costs and capabilities as part of the overall IT lifecycle. This puts DR into the familiar cycle of design, modeling, implementation, monitoring, and optimization (which circles back to design). This breaks them free from a large up-front outlay, and corresponding resource commitment that can include real estate, structures, equipment, and people.

Better yet, it lets them transfer consumables such as power and cooling, software licenses, technology refreshes and upgrades, and other lifecycle costs to service providers.

Because actual demand for DR services—except in case of actual disaster—are likely to be periodic, based on test and audit cycles, and business goal and objectives reviews, they’ll be much less costly on average than the fully burdened overhead costs of setting and managing one’s own DR infrastructure, or paying an MSP to do the job on the organization’s behalf.

Given all the benefits of modern DR and the drawbacks of its traditional counterpart, moving into the Space Age becomes a real no-brainer, doesn’t it?

Once you make that decision, though, what do you do? That’s the subject of the final chapter of this book, in which we look at five of the most important considerations for your backup and DR strategy.
5 Ways to Do DR Better

Rethinking DR for the Future

In the 2020s, approaching DR the same way that organizations have for the last few decades—with human-driven brute force, widespread complexity, and high costs—is going to be a career-limiting move. In fact, IT professionals who want to maneuver their way into a corner office must learn to think very differently about DR.

While legacy strategies for DR may have been cutting edge at the time of their introduction, they’re insufficient to meet the needs of modern business. In a recent survey of 395 IT leaders, 89.6% of respondents indicated that their ability to respond quickly to a disaster has become more important to their organization over the past year. IT users depend on technology more now than ever before. Likewise, the amount of downtime the average business can tolerate grows shorter every year.

At the same time, increasing public cloud adoption has changed the calculus for protecting business data and application workloads. The introduction of VMware Cloud into hyperscale clouds will be the same kind of great equalizer across clouds that vSphere was for data center workloads. Thus, the future is bright for DR planners.

Prudent IT leaders will reflect on the following five considerations when visualizing the future for their DR architectures.

---

1. Don’t Build a DR Site at All

For many years, organizations have built massive IT operations around delivering the technology services their staff and clients need. But recently, there’s been a growing trend of “x as a service” adoption that allows IT leaders to deliver the same value without the overhead and expense of procuring, deploying, operating, and maintaining the infrastructure and software necessary to provide such a service.

A prime example is email. A decade ago, most businesses ran Microsoft Exchange on a physical server in their server room. Today, options like Microsoft Office 365 and G Suite by Google Cloud offer the same—or better—messaging capabilities via a SaaS model. The consumer gets everything they need (email and surrounding features) without all the stuff they don’t need (data center infrastructure, a dedicated Exchange administrator, software support agreements, and so on).

In this new decade, the same paradigm applies to DR. Just like the overhead and inefficiency of running your own messaging infrastructure is almost laughable today, building and maintaining a full DR site that’s propped up by overcomplicated orchestration software is a hopelessly outdated tactic.

Instead, consider adopting a modern approach where DR orchestration is consumed in a SaaS model, and DR infrastructure is only instantiated when it’s needed.

A Secondary Data Center Is Expensive and Burdensome Insurance

Standby data centers are often likened to an insurance policy. They exist for use during a disaster, and only in the event of a disaster. Compared to an on-demand DR site, the costs of maintaining a dedicated DR site are staggering. Consider the following two hypothetical scenarios:

Assume that each business needs to activate their DR plan this year and failover to their DR site.
Business A: Pays multiple six figures per year for facilities, hardware, software, and man hours to deploy and maintain a secondary data center. In the case of a disaster, they pay a few thousand dollars in professional services fees to get hands-on help from their service provider at the colocation facility where their DR site is housed.

Business B: Pays a small fee per year for a software subscription for DR orchestration and the associated storage capacity for backup data. In the event a failover takes place, they pay via consumption-based billing for the computing resources they used, and only for the duration of the outage.

Figure 7 uses the insurance analogy to compare the two scenarios in an easy-to-understand table. While the dedicated DR site has predictably high cost year-round, the on-demand DR site only incurs significant expense during an actual DR event.

The reason progressive organizations love public cloud is because they only pay for what they use, right? Why shouldn’t DR be the same way?
CONSIDERATION #1

For this new decade, consider whether operating a secondary data center and maintaining and testing complex DR orchestration software is really a business you want to be in. Or perhaps you’d be better served by a SaaS orchestration model and on-demand DR service that’s economically and operationally superior.

2. Make Your IT Budget Go Farther and Do More

Your budget is limited, just like everyone else’s. If you could accomplish your backup and DR goals with less budget than you currently allocate and deliver more functionality than you do today, what kind of career-boosting stuff could you accomplish with the budget and time you just freed up?

Beyond just the capital investment in maintaining an entire second data center full of hardware, there are substantial operational costs involved. For instance, think about how much time you spend maintaining software at a DR site. When you patch hypervisors at the primary site, you really should bring the hypervisors at the DR site to the same patch level so you don’t end up with any nasty surprises during a failover. This single, routine task has doubled in scope because of your DR site—and so has the hit to your budget.

Also, what happens if real life got in the way and the DR site wasn’t kept up to date and then you have a disaster? The entire failover plan might not function the way you expect it to, because some component is out of date. Now you’re having a really bad day.
Instead, what if sophisticated SaaS-based DR orchestration software stood up resources entirely on demand? Until you need it, it doesn’t exist; but the moment you need it, it’s provisioned immediately. Now, you never have to spend man hours to maintain it over time. In addition, you know for a fact that it’s not out of date and it’s functional, because it’s brand new and just instantiated.

### CONSIDERATION #2

Envision adopting a new model DR that lets you recover idle and essentially wasted DR funds and put them to work doing exciting things in your organization.

### 3. Gracefully Sidestep Ransomware

You’re more likely to encounter an IT-centric disaster today than ever before. Sure, natural disasters happened in the past and water pipes above data centers broke from time to time. But there weren’t professional crime syndicates out there gunning for your organization’s data to sell on the black market, or trying to hold your data hostage for a ransom. Unfortunately, that’s commonplace today.

Cybersecurity Ventures predicted in a 2018 report that there would be a ransomware attack on businesses every 14 seconds by the end of 2019, and every 11 seconds by 2021.7

There are software solutions available that function like traditional endpoint protection and claim to stop ransomware before it successfully encrypts your data. The fact is that tools like these may prevent some attacks, but you probably can’t rely on them to prevent all attacks.

---

7 Source: “Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021”
In fact, the endpoint security vendor Sophos says in its report that 77% of organizations surveyed who were victims of ransomware attacks were running up-to-date endpoint security at the time of the attack.8

Bad guy ransomware developers will continue to innovate just as fast as the good guys do, and while you may be protected against weeks-old ransomware strains, it’s likely that there will be zero-day exploits and

Figure 8: One need not even develop their own ransomware today; ransomware as a service (RaaS) is a burgeoning business and is growing rapidly. Some developers offer affiliate programs where novice cybercriminals don’t even have to front any cash for the software. Others sell complete ransomware toolkits with maintenance for as little as a few hundred bucks.

8 Source: “The State of Endpoint Security Today,” 2018
ransomware that behaves in new and unforeseen ways that slip past defenses. With the appearance of ransomware as a service business models over the past few years, the threat of ransomware is growing exponentially (see Figure 8 for how it works).

Running advanced endpoint protection systems is absolutely a good idea, and should be standard practice. But endpoint protection alone isn’t enough; you need to have a fallback plan for when ransomware slips past your first line of defense.

Why has the ability to respond quickly to a disaster become more important?

- Increasing threat of ransomware: 70.1%
- Increasing threat of power outages: 55.4%
- Increasing threat of human error: 52.3%
- Increasing threat of natural disaster: 50.8%
- Increasing impact of downtime on the business: 70.1%

**Figure 9: Ransomware is the top reason that IT professionals are seeking a lower recovery time**
When ransomware touches your organization, you’re going to have business leaders breathing down your neck. They’ll be asking for status updates and pressuring you for an ETA on getting systems back up (Figure 9). The only thing you’ll really care about in that moment is RTO—how quickly you can recover.

**Give Ransomware the Boot**

Ransomware is getting smarter all the time, and plenty of ransomware strains now go after your backup data, too. But as sophisticated as ransomware has become, it’s actually a relatively small blip on the radar when you’ve got a backup and recovery strategy that’s more sophisticated.

For a solid recovery plan to defeat ransomware, you want to be working with immutable backup data. Immutable means that once your backup data is written, it’s literally impossible to modify it. Future versions of that data are copies, but the original still exists in an unadulterated form.

Here’s a recipe for painless ransomware recovery: Combine a backup tool with a high level of granularity when it comes to restore points with one that leverages an isolated namespace with immutable backups for retention. Mix in a tightly coupled DR orchestrator that can easily bring your business back online at a DR site from a healthy snapshot, along with a backup system that can instantly restart the applications so that rehydration doesn’t take days, and you’re set.

**CONSIDERATION #3**

Be prepared to outmaneuver ransomware. Not only do you not even need to consider paying the ransom, you also don’t have to spend days or weeks recovering. You simply choose the restore point, revert to that point in time, and pick up where you left off.
4. Backups Are Ineffective; Focus on Recovery

It’s been said that “If your data doesn’t exist in at least two places, then it doesn’t exist.” The sentiment behind that statement is a good one, but, unfortunately, it doesn’t go far enough. Beyond needing to just ensure that you back up your data, it’s also of paramount importance that you know beyond a shadow of a doubt that you can recover from your backups.

Just as it’s impossible to know the fate of Schrödinger’s poor cat until you open the box, it’s impossible to know whether your backups will save you until you actually restore them to production. And when it comes to DR, you don’t know that your failover will be successful until you actually push the button. If you test your DR plans regularly, you can have this level of confidence; unfortunately, most organizations don’t test regularly enough to be sure (Figure 10).

<table>
<thead>
<tr>
<th>How Often DR Plans Are Tested</th>
</tr>
</thead>
<tbody>
<tr>
<td>28.9%</td>
</tr>
<tr>
<td>28.4%</td>
</tr>
<tr>
<td>23.5%</td>
</tr>
<tr>
<td>12.4%</td>
</tr>
<tr>
<td>4.3%</td>
</tr>
<tr>
<td>1.3%</td>
</tr>
<tr>
<td>1.3%</td>
</tr>
</tbody>
</table>

Figure 10: Nearly three-fourths of survey respondents aren’t testing their DR plans monthly
You Performed a Successful Failover? Great!
Now Can You Fail Back?

Plenty of DR products on the market excel at orchestrating a failover and getting your DR site online quickly. If they’re tested regularly, they may solve your initial problem of bringing the business back online. But failing over is only half the battle. Where many DR solutions fall flat today is when it comes time to fail back to the primary site.

It turns out that diverting production traffic back to the primary site is a little trickier than you’d hope. Consider some of the ways that failback can go sideways (Figure 11):

- If there was a VM format conversion in order to fail over, you’ll need to convert back to the original format again. In the best
case, that process will probably take more time than you’d like. But as anyone with experience doing physical-to-virtual or virtual-to-virtual migrations will tell you, expecting a system to go through two machine format conversions and come back up with no issues is a long shot at best.

- Replicating back the changed data can become an expensive proposition if you’re coming back out of a cloud; egress charges can add up quickly if you aren’t judicious about how to reflect the changed data back to the primary site.

- Some cloud providers have tools that can help with failover, and that’s great. They have very little incentive to help with your failback, however. It could be argued that they don’t even want you to fail back successfully.

5. Have Faith in Your DR Plan

We’ve reached a point in the maturity of DR technology where you don’t have to make the trade-offs you were forced to make even just a few years ago. Today, it truly is possible to have your cake and eat it too.

Don’t Settle on Your Recovery Objectives

One of the most significant ways that DR technology has matured is in its ability to deliver a reliably low RTO and RPO.

CONSIDERATION #4

When it comes to DR, focus on the key word: recovery. Backups are a crucial part of the picture, but legacy backup technology often falls flat when it comes to recovery time. Additionally, look at a modern approach to failover and failback.
Avoid Committing to a “Mostly Achievable” RTO
When it comes to responding to a disaster, one could argue that no variable is more important than recovery time (Figure 12). You can sort out everything else later; but while the organization is unable to function, the only thing that matters is restoring functionality quickly.

Many businesses today don’t even know what recovery time they’re capable of. Those that do have some idea—either from experience or from their careful estimates—may have RTOs that are many hours to many days in length. It’s not uncommon to hear of RTOs measured in weeks. These businesses are forced to sit and wait while backup data is rehydrated and VM conversions are completed. There’s just no reason to settle for this anymore.

When the organization is crippled and infrastructure is down hard for many days, that’s bad for business. There’s DR technology available today that can easily meet a four-hour SLA—and it’s not outlandishly expensive. In fact, it’s possible today to achieve an RTO that’s measured in blinks of an eye—in other words, nearly zero.

Respondents ranked the following DR solutions in order of importance:

1. Recovery time objective (RTO)
2. Ease of use
3. Ease of failback from DR location
4. Ability to keep VMs in their native format
5. Recovery point objective (RPO)

Figure 12: Survey respondents ranked Recovery Time Objective as the most critical factor in choosing a DR solution
An ‘OK’ RPO Is Not OK
If you’re using legacy backup and DR software, you’re likely measuring RPO in hours on the low end and days if you’re closer to average. When you run weekly full backups and nightly incrementals, you’re really leaving valuable RPO time on the table in the 2020s. There’s technology available now that can improve your recovery granularity to increments as small as five minutes.

Don’t Accept Operational Inconsistency During Crisis
Primarily for fiscal reasons, it’s not uncommon for the primary and secondary data centers to be heterogeneous. Different hardware, different software, different architectures. Unfortunately, skimping in this area can seriously backfire.

When a disaster strikes, the last thing you want to see is your team grasping at straws, trying to figure out how to operate the unfamiliar infrastructure at the DR site.

Of course, some organizations can justify spending enough to create a mirror image of the primary data center at the secondary location. This does solve the problem of inconsistency, but it’s wildly inefficient financially.

Fortunately, there’s a third option for DR in the 2020s. By leveraging VMware Cloud on AWS to create an on-demand software-defined data center (SDDC) when and only when you need it, it’s possible to create a DR site that uses the same vSphere interface that your team uses at the primary site and only pay for that infrastructure when it’s in use.

For somewhat relaxed SLAs, a VMware SDDC can be provisioned in 90 minutes or less, and VMs can start coming online at the DR site in less than two hours. For those with tighter SLAs, there’s a pilot light configuration where the SDDC is already provisioned and your first critical VMs can start coming online in five minutes.
This third option offers the best of both worlds: It easily fits within modest DR budgets, but also affords administrators the luxury of a homogenous user experience between the primary and DR sites.

**Don't Accept Runbook Fragility**

Many DR runbooks involve lots of manual steps that humans must perform. When those humans are under immense pressure, those steps can be especially error-prone. Further, most automated DR runbooks in use today are somewhat brittle. If everything doesn’t go exactly according to plan, your failover bombs. And during a major outage is precisely the time you *do not* want to be working out kinks in the system.

The inoculation is to perform regular failover testing. And while that sounds relatively simple, it has historically been anything but. Not so long ago, it was common practice to schedule full teams of IT staff to run through DR simulations over the weekend (causing an outage to the production environment) to make sure that all systems were recoverable as expected.

Today, however, this sort of large-scale wargame is wholly unnecessary. The technology exists today to simulate a failover event in a sandbox in the middle of the business day with your users none the wiser. Your DR vendor may even include a block of hours to allow you to conduct failover testing without incurring any additional fees. You can validate your failover capability at any time, and confidently tell your boss and your auditors that you can meet your SLAs.

**Don't Overcomplicate Things**

Traditionally, backup was a standalone product. Replication and DR was a second, independent product. Both of those interfaced with your storage platform(s), which was yet another different product. If data security was a concern—and where isn’t it?—then encryption software
was often a separate product (which interfered with storage efficiency and WAN optimization, by the way). You get the point.

In a DoorDash world where we can’t even be bothered to get off the couch to get our own dinner, there’s an expectation that IT shouldn’t be such a Rube Goldberg machine. There should be a unified platform for all data functions. As we take on the 2020s, it’s realistic to expect a single platform to manage primary storage, backups, DR, encryption, and mobility.

Quick quiz: What happens in a troubleshooting scenario when you have five different vendors involved? You know what happens—they all point fingers at each other and no one does anything, meanwhile you’re down hard and your boss just kicked a trash can across the room.

Having a single point of support for primary storage, backup, and DR means that when disaster strikes, you’re going to actually call a vendor who’s got your back and you’re going to get help right away.

CONSIDERATION #5

Modern DR for this new decade should be simple, reliable, and provide operational consistency during a failover event. Aggressive RTOs and RPOs are in reach for most organizations today and you shouldn’t settle for anything less than what the business needs.

Do Disaster Recovery Better

So, to summarize, here are the five ways you can do DR better this decade.

1. **Don’t use a DR site at all.** Instead, leverage the on-demand capacity of VMware Cloud on AWS to spin up temporary DR resources only in the event that you need them.
2. **Maximize your budget’s potential.** By recovering funds from unnecessarily expensive DR initiatives, you can tackle all sorts of new and exciting projects.

3. **Say “No” to paying ransoms.** With the right converged backup and DR technology in place, there is no need to engage in a power struggle with ransomware developers. Instantly restore to just before the attack, plug up whatever hole they came in through, and move on about your business.

4. **Focus on recovery.** The best backups in the world fall down when it comes to DR, unless the system is optimized for recovery speed. Many top–of–the–line backup products are fantastic at storing backups and archiving data; but they fail you at precisely the moment you need them most, which is during DR, by taking hours or days to rehydrate data and perform VM conversions in the cloud.

5. **Believe in your DR plan.** With the right technology foundation, you can implement a DR plan free from the staleness and fragility characteristic of many DR plans. With regular, verified recovery compliance, you can actually have faith in the integrity of your DR plan.

**Survival of the Modern**

This Gorilla Guide has taken you on a journey through backup and disaster recovery: its past, present, and future. As you’ve seen, legacy solutions just aren’t equipped to meet today’s needs for fast recovery of your precious data. Emerging threats call for more resiliency, and business can’t wait a day, a week, or even longer to restore operations anymore. Time is money in the Internet age, and extended outages are no longer an option.

But there is hope. Leveraging the power of the cloud provides avenues of swift recovery, and strengthens your ability to respond to disasters, whether natural or manmade. DRaaS is growing in
popularity—offloading the hard stuff to experts is appealing for many organizations today, and makes financial sense both in terms of CapEx costs and the cost of extended downtime.

That’s why the future is clear: To do backup and DR in the modern era requires modern tools and methods. Getting left behind can affect more than your short-term bottom line—it can affect your organization’s very survival.