



A New Approach to **Disaster Recovery for a New Era**

The dramatic changes in how, where and when employees work have brought about an intense need for organizations to update and, in many cases, overhaul their approach to risk management, especially disaster recovery. Specifically, new strategies, processes and solutions are needed to account for dramatic changes in workforce deployment. This paper talks about problems, implications and opportunities for disaster recovery in a rapidly changing landscape.

Since the outbreak of the global pandemic, the term “disaster recovery” has taken on an entirely new meaning. But the dramatic shifts in enterprise workforce deployment have brought with them substantial realignment in IT disaster recovery (DR) from testing to actual recovery of core IT assets, such as systems, applications and data.

In the pre-COVID-19 era, DR testing was carried out by a team of technical specialists who traveled to the off-site recovery center, where they implemented the steps identified in the organization’s DR plan. Those teams’ goals included determining if they could meet pre-determined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), as well as ensuring that proper failover occurred and that systems and data were fully recovered.



COVID-19 not only changed how DR testing and recovery was done in the short term, but it is likely to be very different even when the pandemic eases and organizations start to revert to “normal” operations. Without question, more and more employees will continue to work from home or other remote locations—some on a part-time basis, but many of them on a permanent basis. This has dramatic implications for how DR—from testing to actual recovery after an unanticipated event—will be planned, implemented and managed.

Failure to take into account the need for new DR protocols and solutions has numerous significant implications, from potential compliance violations and data governance challenges to catastrophic financial loss, deterioration of brand reputation and an irrevocably diminished customer experience. With the average hourly cost of downtime now pegged at \$260,000, the stakes have never been higher.¹

HOW DISASTER RECOVERY HAS CHANGED

Over the past decade, DR has become increasingly critical in direct relationship to the growing importance of data, applications and all digital assets. The increased reliance on technology among organizations, their customers and their entire business ecosystem means that keeping systems up and running is of paramount importance. When unplanned outages do occur, getting systems back up and having data restored to its most recent known state can mean the difference between a successful organization and a defunct one.

Now, with the increasing move to remote work as a result of the COVID-19 pandemic and the undoubtedly lasting reliance on mobility and remote digital resources, organizations need to take a new look at their DR strategies, tactics and tools. For instance, testing will need to be done remotely in many cases, with fewer DR-related personnel able (or willing) to travel to remote sites. Additionally, access to office and data center security controls is likely to be limited, as will access to legacy data center-delivered systems interfaces, enterprise-class networking performance and multifactor authentication tools and methods.

The pandemic, and the increased utilization of consumer-class devices in home settings, have brought with them a dramatic increase in cyberthreats, including mobile malware, phishing and ransomware. This has dramatically increased threat vectors as well as created a heightened sense of urgency to detect, protect and defend against sources for data breaches, service outages and costly downtime.

It also is clear that using remote locations for DR and fail-safe operations means that distance-induced latency is more challenging than ever, putting more pressure on organizations to account for latency reduction in their DR plans. Also, there are more infrastructure “choke points” that contribute to DR complexity, such as widespread virtual infrastructure, VM sprawl, physical server growth and an accelerating need for data protection in the face of astonishing data volume growth on storage systems. Finally, the widespread move to digital transformation means that digital assets are literally the lifeblood of the organization, putting added pressure on enterprises to wall off threats of service interruptions and, when outages do occur, to recover immediately and fully.

¹ “Stat of the Week: The (Rising!) Cost of Downtime,” Aberdeen, April 21, 2016.

REDEFINING AND RE-ARCHITECTING YOUR DR STRATEGY

New DR methods and solutions are necessary to overcome the challenges of these dramatic changes in workforce deployment, as well as to ensure reliable, instantaneous and documented failover and recovery. Although nearly all enterprises have some kind of DR plan in place—if not always in a ready-to-go state—many organizations designed those DR plans years ago, before the dramatic impact of such new developments as the primacy of cloud computing, “as-a-service” IT models, widespread mobility, new cyberthreats and the “new normal” of remote work.

This means that DR plans must be updated and, perhaps, overhauled to include a wide range of new capabilities. These include:

- The ability to dramatically reduce latency and improve responsiveness as geographic coverage areas increase.
- The twin realities of dispersion and proximity, where digital assets are increasingly distributed, mean DR solutions must enable greater proximity to applications, systems and data for fast recovery.
- Accounting for mobility and remote access as integral to the overall DR strategy.
- Coverage from the data center to the edge to the cloud and back.
- DR as part of an overall business continuity framework, which, in turn, is part of a comprehensive risk management approach that is tightly tied to core business objectives.
- The ability to aggregate services seamlessly and efficiently to restore real-time access to all digital “junctions,” such as cloud services providers, SaaS vendors, carriers, business partners, supply chain participants and more.

- Trusted and secure access methods for remote workers.
- Provider-neutral, centralized key management with multisite and hybrid cloud support, including support for single enterprise-wide keys across cloud and IT data centers.
- Optional dedicated on-premises hardware for workloads that cannot be confidently and securely deployed in the cloud.
- Creating a flexible recovery and production environment that is aligned with each organization’s unique goals and circumstances.
- Tighter collaboration, trust and partnership with IT services providers that can ensure reliability, security, scalability and recoverability from the edge to the core.

WORKING WITH EQUINIX ON A MODERNIZED DR FRAMEWORK

Disaster recovery solutions are typically unique to each organization’s specific circumstances, including legacy infrastructure, RTOs/RPOs, business challenges, carrier/service provider relationships and cost-versus-risk thresholds. That puts a premium on finding a technology partner with a DR solutions portfolio that is both wide and deep.

Equinix, the world’s digital infrastructure company, offers enterprises a wide array of DR solutions that can be planned, deployed and managed with each organization’s unique needs in mind. Equinix not only offers the industry’s leading portfolio of physical and virtual infrastructure solutions, but it also meets the business needs of organizations with advanced virtual consumption options for foundational server, networking, monitoring and security capabilities. It offers the broadest global footprint of locations and the most direct on-ramps to the public cloud, with software-defined connectivity to thousands of partners and providers to help businesses seize opportunity with agility, speed and confidence.

The Equinix DR solutions include:

- [Equinix Internet Exchange™](#), a global platform that helps organizations establish and maintain reliable, consistent interconnections around the world, optimizing the management of content, network infrastructure, application performance, edge-based distributed data and IoT/big data demands.
- [Equinix Cross Connect](#), which delivers high-performance, low-latency and highly secure network connections through a global network of Equinix data centers enabling interconnections across carriers and service providers.
- [Equinix Fabric™ for cloud-based DR](#), which connects digital infrastructure and services at software speed. Built specifically for digital infrastructure, Equinix Fabric enables businesses to connect globally to their choice of thousands of networking, storage, compute and application service providers in the industry's largest infrastructure ecosystem.
- [SmartKey® for centralized key management](#), a cloud-ready way to manage keys, encryptions and tokens as a service and to protect data in public, private, hybrid and multicloud environments.
- [Network Edge](#), a software-defined network automation tool that acts as an edge instance for use cases where key requirements are essential, such as time to market, proximity of major content and enterprise services, and minimized touch points.
- [Equinix Metal™](#), which helps organizations quickly and securely deploy physical infrastructure across global locations. This bare metal as a service is fully programmable, easy to use and ready to scale—close to networks, clouds, users and ecosystems.

Finally, Equinix has a unique and market-proven ability to act as a trusted partner in advising customers on how to design and deploy disaster recovery as part of an overarching business continuity and risk management strategy.

CONCLUSION

Reducing and, where possible, eliminating downtime is critical in today's digital economy. But legacy DR approaches were often built in an era when issues such as hybrid cloud/multicloud environments, edge computing and pervasive, sophisticated cyber threats were less prevalent than they are today.

In this era of digital transformation, marked by widespread mobility, global collaboration, always-on connectivity and remote work, new approaches to DR are essential. That's why organizations need to look for technology partners that not only can bring a fresh and expansive view of DR to the table, but also can demonstrate a proven record in helping organizations identify, minimize and remediate the impact of risks to system and application availability.

Equinix has a long history of market leadership in global interconnection solutions, combined with a demonstrated ability to act as a valued business partner for organizations with complex digital ecosystems. Equinix's peering-point advantages and its breadth of flexible edge options makes the company an excellent option for organizations looking to modernize their approach to DR.

[Learn more](#) about how Equinix is helping enterprises architect DR plans that ensure applications recover quickly when needed and continue to provide seamless services to end users.