



RETHINKING DISASTER RECOVERY:

The Impact of Cloud Computing

A Bryhtpath LLC White Paper



EXECUTIVE SUMMARY

Developing new strategies to reduce IT service disruptions without increasing costs is a challenge plaguing many organizations across multiple industries. Traditional solutions to enhance business continuity—such as storage, server, and perhaps data center redundancy—were often the only available options that could satisfy the rigorous resilience objectives of most major corporations. However, these systems tend to be expensive and they still leave the organization highly vulnerable to system failures.

As businesses begin to adapt to a constantly evolving, global marketplace, leaders expect a long-term continuity strategy that supports service delivery regardless of the location. In addition, organizations want a long-range strategy for reducing recovery times in the event of a service disruption, system outage, or natural disaster.

Transitioning an existing Disaster Recovery Plan (DRP) to a cloud environment can resolve these problems while offering a multitude of additional benefits that many organizations rarely consider. For example, a cloud-enhanced DRP allows businesses to add or remove resources and services as needed while paying only for what they use at any given time. By transitioning business continuity objectives to the cloud, organizations become more agile, flexible, and easily scalable to grow and expand along with their business.

However, a successful transition requires a well-planned approach and a thorough understanding of cloud computing. There are several considerations to address before creating a transitional strategy to a cloud-based environment, including service-level agreements (SLAs), integration with traditional disaster recovery methods, and offsite storage feasibility.

This white paper examines the resiliency challenges facing organizations today and discusses the factors that organizations must address. The paper also presents a step-by-step approach for planning, designing, implementing and evaluating the transition to a cloud-based disaster recovery strategy.

The Changing Landscape of Disaster Recovery

Many leaders mistakenly assume that the threats of service disruptions will automatically decline as technology continues to advance. In reality, the reverse is true. For example, in a recent study by the Aberdeen Group, statistics show a [38% increase in downtime](#) occurrences between June 2010 and February 2012.^[i] As businesses continue to become more automated, they also have fewer people visually monitoring the business continuity systems throughout the day. As a result, disaster seemingly strikes without any advanced notice, and the IT infrastructure comes to a complete standstill.

Aberdeen estimates the average cost-per-hour of a typical service disruption to be around \$182,000. For larger organizations with multiple office locations, the financial losses for this excessive downtime can soar into the millions of dollars annually. Furthermore, a 2012 IBM study entitled [Reputational Risk and IT](#) identifies system outages as one of the top two IT-related challenges that can also do severe damage to a company's professional reputation.^[ii] Several factors contribute to this new trend:

- **Rise in software applications**

The number of software applications that organizations utilize is increasing at an alarming rate. It costs companies a great deal of money for the associated hardware and technical management of all of these applications as well. Additionally, the proliferation of applications also leads to an increase in the system's potential points of vulnerability.

- **Virtualization is more appealing**

To reduce costs, companies are taking advantage of virtualization more frequently. However, when virtualized machines and applications are not properly managed, important information may be lost both before, during, and after the transition.

- **Falling costs of hardware**

The individual hardware components involved in a traditional DRP are now more inexpensive, which leads many companies to postpone transitioning to the cloud. Even though they may want to maintain backup and recovery systems in-house, very few of today's enterprises have the technical expertise, skills, or regimented discipline required to manage these in-house protocols effectively.

- **A workforce and customer base on the move**


Organizations today have both employees and customers who access the IT infrastructure from smartphones, home offices, field offices, and hotel rooms located in nearly every geographical region on the planet. Although companies tend to spend a great deal of money on their IT infrastructure, poor performance and spotty service availability are issues that are beyond their control.

Even as the marketplace continues to become increasingly competitive, the technology itself is advancing at a rapid rate. Companies not only find it difficult to keep current, but they are also spending more of their annual budgets on their software applications, hardware, and management processes required to remain competitive. Organizations are under constant pressure to “do more with less.” As a result, monies spent on internal DRPs and business continuity systems are dropping each year, even though the demands being placed on the business are escalating.

Organizations are now required to operate in mixed environments and around the clock while supporting multiple internal key objectives of an effective Disaster Recovery System, including:

- Manage and resolve ongoing capacity and skills shortages.
- Provide high-quality and accurate data that is immediately available 24/7.
- Develop and implement business continuity strategies during downtimes and data outages
- Facilitate faster recovery from interruptions or disruptions.
- Secure skilled technicians to manage the data recovery and backup in-house.

The perceived and actual risks are also increasing. According to a recent [Forrester Research and Disaster Recovery Journal](#) survey, 82% of business continuity decision-makers feel that their company’s risk level for service disruptions and data loss is increasing at a consistent rate due to a variety of reasons, including:

1. Business complexity
2. Reliance on technology
3. Intensity and frequency of natural disasters
4. Reliance on third parties 

Common Misconceptions about Disaster Recovery

People tend to fear change. This fear of the unknown is one of the primary reasons why so many organizations are slow to transition to a cloud-enhanced DRP and business continuity plan. But service disruptions do not discriminate. Just because a particular enterprise has remained disaster-free in recent years does not mean that the existing DRP is still appropriate. Many companies automatically assume that their existing DRP is in perfect working order simply because they tested it five or ten years ago and found it to be effective. Unfortunately, these are the companies that are probably the most vulnerable to a disaster.

A well-planned and easy-to-execute DRP can mean the difference between life and death for a business. Luckily, there are many examples of major companies facing a catastrophic service disruption head-on without skipping a beat. A service outage doesn't have to be detrimental. It all depends on the company's DRP strategies and capabilities. People, technology, timing, and resource availability all play a crucial role.

There are [four primary misconceptions](#) that organizations have about DRPs that often result in a company continuously postponing a re-evaluation of their existing disaster recovery strategies. [\[iv\]](#)

1. *"We already have a DRP in place."*

Having a Disaster Recovery Plan in place does not mean that the organization is fully protected. When was the DRP initially created and tested? What new changes in internal systems, technological hardware, and software applications has the company undergone since the DRP's initial implementation? What changes to strategic objectives, organizational structures, or other factors have occurred since the DRP's initial implementation? A DRP solution can only provide full protection when the organization implements a holistic approach that accounts for every area of business continuity. The solution must also be thoroughly tested for possible planned and unplanned disaster scenarios.

If the existing DRP works but offers no method to communicate the disaster related implications for the end users, then the DRP is essentially worthless. The business experiences the same negative impacts as not having a DRP in place at all. Furthermore, implementing a DRP solution without extensive testing means that the organization will not discover the inevitable glitches in the system until it is far too late.

Planning for a potentially disastrous power outage is only one of the major factors. It is the unplanned and uncontrollable disasters that can keep company executives up at night. What would happen to your DRP if certain resources were unavailable? What if the disaster is so

severe that employees would rather run home to check on their loved ones that sit around the office trying to get the IT infrastructure up and running again? What happens if the company's traditional backup tapes fail to restore, for whatever imaginable or unimaginable reason?

For a DRP to be deemed successful and effective, no assumptions should be made regarding availability of individual resources or infrastructural components. Furthermore, if testing the DRP takes too long or negatively impacts business productivity too much, then the current DRP is not the best solution. It's time to update the DRP.

Example Disaster Scenario: Company providing mobile services experiences system failure.

Smartphone owners know this scenario well. A snowstorm knocks down a cell tower clear across the state, causing a million customers to lose cell service instantly. If the snowstorm lasts for several days, like recent New England experiences, customers can get quite nasty very quickly without their phone service. As a result, the mobile service provider might issue an official press release stating, *"We are sorry for the inconvenience, but our service relies on several different components, applications, and systems. We will do our very best to restore services promptly."* Meanwhile, tens of thousands of customers are jumping online, searching for a new phone plan from a different and more reliable company. Not having an effective DRP plan can ruin a company's reputation, even if the disaster is outside of their control.

2. "All you need for a DRP plan is a really good back-up generator."

A backup generator might seem like an effect DRP solution for smaller companies concerned only with local availability of the company network. Unfortunately, it is not that easy. One of the primary objectives of an effective DRP is to remove as many single points of failure as possible, including individual sources of data, individual connection points, and individual power grids. A generator gives the company a temporary source of power, but it also requires regular maintenance and an instantly and always available fuel source. Remember, any mechanical device can simply refuse to start for a variety of reasons. If the company gets hit by a huge flood, will that gasoline-powered generator work underwater?

Example: Northern Virginia loses 911 service for 2.3 million people

In July of 2012, a severe thunderstorm hit Northern Virginia just outside of Washington, DC. Verizon officials told government leaders that the backup generator and the backup-backup generator simply would not start. The result was [2.3 million](#) people losing Emergency 911 Services for four days, and another one million businesses and private citizens being without electrical power 

3. “We haven’t had an outage in years. We’ve got more critical issues to solve first.”

Technology is advancing so rapidly that many IT organizations postpone updating their DRP until all new systems, hardware, and software are in place and operating smoothly. Unfortunately, this is a process that never ends. The business, its customers, and its professional image are at stake. Investing in an up-to-date, cloud-based DRP may not seem critical to many organizations, but should be proactive than reactive.

Example: After a period of three years without disruption, a CRM provider experiences two outages in two weeks.

This company had a DRP in place that focused on advanced separate instance redundancy, but there were no contingency plans in place in cases of failover. The first outage occurred from a tier storage issue. The second from a standard power failure. Without a contingency plan, the organization comes to a complete stop twice in two weeks until the issues were resolved. Every mishap provides the company with an opportunity to learn something new about their IT infrastructure and DRP plan. Don’t be lulled into a false sense of security, mistakenly believing that disasters always happen to the other guy.

4. “Unlike most companies, we actually have a secondary Disaster Relief Site located completely off-property.”

One of the older approaches to disaster recovery is to implement a system that involves a separate, secondary location somewhere off-property that can be pulled into action rather quickly in cases of emergency. The idea behind a secondary DRP site is that the company can still function if the primary offices are hit by a natural disaster, like a hurricane, fire, flood, or tornado.

However, most organizations choose a secondary DRP site that is in close proximity to their primary office space, which only makes sense because a team of employees would have to be able to access the site relatively quickly from the primary location. Unfortunately, if the company’s main offices are hit by a natural disaster, then the secondary location probably becomes a victim as well. Even in cases of a regional power outage or blackout, the secondary DRP tends to fall on the same grid.

Considering these changing environment and misconceptions, transitioning an organization's DRP to a more cloud-friendly environment can eliminate a great deal of the potentially negative consequences from unplanned disasters. The initial investment of time and money for a world-class disaster recovery strategy may seem difficult to justify, especially during periods of economic hardship, but a truly effective DRP will pay for itself ten times over once the company faces its very first service disruption. The ability for the business applications to function 24-hours a day and 365-days a year boosts customer satisfaction levels, client relationships, employee morale, and the brand name reputation of the enterprise.

Traditional Disaster Recovery: Dedicated versus Shared

In traditional disaster recovery models, including both dedicated and shared options, organizations often feel as if they need to choose between cost and speed of recovery. When choosing an approach to design their DRP solution, companies have typically focused on the desired level of service required, as measured by two recovery objectives:

- **Recovery Point Objective (RPO)**

The point in time where data is restored and reflects the amount of data that will be ultimately lost during the recovery process.

- **Recovery Time Objective (RTO)**

The amount of time between an outage and the complete restoration of operations.

In a dedicated model of disaster recovery, the DRP is dedicated to a single organization, which usually results in a faster time to recovery compared to other traditional models. The IT infrastructure is duplicated or mirrored at the secondary disaster recovery site and is ready to be quickly pulled into action in the event of a disaster.

While a dedicated model can reduce RTO because the hardware and software are preconfigured, it does not eliminate all related delays. The process is still dependent on the physical transportation of backup tapes and a somewhat involved data restoration process. This approach is also costly because the secondary infrastructure sits idle when not in use for disaster recovery. Similarly, a multi-datacenter high-availability (MDHA) solution is also quite expensive.

In a shared model of disaster recovery, the secondary infrastructure located off-site is shared among multiple organizations, which tends to make it more cost effective. When a disaster occurs, the hardware, application software, and operating system at the secondary site must be configured from the ground up to match the home organization's IT infrastructure currently experiencing the disaster. Configuring a system from scratch can take days or even weeks. Meanwhile, the organization still has to worry about the lengthy data restoration process just like with the dedicated model. As a result, the shared model is a bit less costly, but it takes far more time to employ.

The Pressure for 24/7 Availability

A common challenge facing organizations today is the need to keep up with the growing demands on their IT departments while maintaining the continuous efficiency of business operations. Both users and customers are now more technologically sophisticated as usage of Internet-connected devices is growing by leaps and bounds. Meanwhile, corporate IT budgets remain relatively unchanged from year to year. Even though this pressure for 24/7 availability is increasing, organizations are spending tremendous amounts of time, money, and other resources simply to maintain their existing systems. There's nothing left for the new upgrades.

When deciding between the traditional disaster recovery solutions of either dedicated and shared models, organizations are essentially forced to choose between cost and speed. As the pressure to achieve continuous availability and reduce costs continues to intensify, organizations can no longer accept the cost and speed tradeoffs of traditional systems.

While traditional DRPs were originally intended for critical emergencies of "Acts of God," many organizations today are now demanding real-time recovery solutions because their online presence is the primary interface with their customers. Any disruption in service, not just natural disasters, reflects poorly on the company image. Interruptions of key applications such as online payment processing, purchasing, or other forms of customer self-service are viewed as unacceptable. A single minute of downtime can cost the company tens of thousands of dollars and perhaps hundreds of previously loyal customers.

A New Definition of “Disaster”

Only a few, short years ago, IT administrators would declare a disaster only in cases of extreme events, such as hurricanes, floods, fires, and hurricanes. Today, even the most mundane service destruction can have a catastrophic effect on the company’s profitability and brand name reputation. Therefore, instead of planning for the “worst case” scenarios, organizations are now planning for the “most likely” when developing and implementing their DRP, such as cut power lines, server failures, or breaches in security.

Traditionally, the most common causes of data loss include:

- **Network and system failures**
All computers, hard drives, servers, and individual components of a company’s architectural infrastructure have a pre-defined lifespan. They do not last forever. Without proper maintenance and regularly scheduled system reviews, something is bound to break down sooner or later.
- **Application failures**
Most every end user has experienced the occasional software or application failure. For no apparent reason, it simply stops working, perhaps due to a corrupted file, a software upgrade that did not fully install, or the utilization of a certain diagnostic tool that requires too much memory.
- **Network intrusions**
Viruses, malware, and ransomware are just a few of the unwanted network intrusions that can lead to lost or corrupted data. Even though most companies utilize some sort of anti-virus protection software, these programs are not 100% foolproof.
- **Malicious attacks from cybercriminals**
No organization is exempt from a cyber-attack. Even if the company manufactures the most insignificant contraption known to man, cybercriminals don’t need a reason to hack into a company network. They do it just for the sheer enjoyment.
- **Power failures**
Power failures come in many forms, including regional electrical blackouts, disruptions in Internet service, or even a lightning strike to the building housing the IT servers. Even a healthy power surge of electricity, which are extremely common, can cause minor disruptions that can easily lead to lost data.

The New Approach: Cloud-based Business Continuity

Cloud computing offers an attractive alternative to traditional disaster recovery. “The Cloud” is characteristically a shared infrastructure. The associated costs of its resources are essentially distributed across any person or organization that contracts with the cloud service provider.

This new form of shared model is ideal for disaster recovery. Even when the definition of disaster recovery is redefined to include more mundane service interruptions, the need for disaster recovery resources is still somewhat erratic. Since it is very unlikely that every organization contracting with the cloud service for backup and recovery will undergo a disaster at the same time, the costs can be significantly reduced overall, and the cloud can speed recovery time for everyone involved.

Managed services for cloud-based business continuity are designed to provide the perfect balance of cost-effective, shared disaster recovery models with the speed of a dedicated infrastructure. Because the cloud-stored data is continuously replicated, recovery time can be reduced substantially to less than an hour, and in some cases, a matter of mere seconds. Meanwhile, the associated costs are more consistent with a shared recovery system. While cost and speed are important considerations, there are several other benefits to a cloud-based disaster recovery plan:

- **Reduced up-front costs**

Designing, deploying, and managing a traditional DRP can be a very complex process, requiring time, money, and staffing. Transitioning to a cloud-based DRP typically does not require massive expenditures for special hardware, the hiring of new technical specialists, or an additional investment in a secondary site located off-property.


- **Predictable budgeting**

Traditional DRP solutions can force some companies to make tradeoffs regarding what the company can *afford* to protect versus what the company *should* protect, which can leave the organization extremely vulnerable. The associated costs to manage traditional models can also be somewhat sporadic. With a cloud-based DRP, companies benefit from more predictable operating expenses that are also easily scalable to grow and expand along with business needs.

- **No secondary site required**

Cloud-based DRPs offer portal access with failover and failback capabilities, which eliminates the need for a secondary disaster recovery site located somewhere off-property. The DRP can be put into action from any location with Internet access, which also eliminates the costs associated with travel time to the secondary site as well as its regular maintenance and upkeep.

- **Improved data protection**

With the number of corporate data breaches dramatically increasing in recent years, it has become paramount for companies of all sizes to have a strategy in place for backing up data to multiple locations that are quickly and easily recoverable. According to [Symantec's 2015 Internet Security Report](#), the total number of data breaches increased by 32% in 2014, or about 312 more than the previous year.  As cybercriminals become increasingly inventive, organizations need to test their DRPs more frequently. Cloud-based DRPs make testing far easier than with traditional models.

- **Simplified Process for Disaster Recovery**

Traditional DRP models require the company to hire a staff member who will be responsible for managing, updating, and implementing the disaster recovery process on an ongoing basis. Once a disaster is declared, the company must rely on perhaps a single employee to get the system back up and running. Cloud-based models are infinitely easier to put into action, essentially streamlining the entire disaster recovery process from start to finish. However, they can also be designed to coexist easily with traditional recovery models to provide the company with increased flexibility and support.

20 More Reasons for Cloud-based Disaster Recovery

A recent Forbes magazine article recently noted more than 60% of businesses will have at least 50% of their IT infrastructure located on cloud-based platforms by the year 2018.^[vii] There are many reasons driving this surge in popularity to switch to a cloud-based disaster recovery solution. Traditionally, backup and archiving procedures have been a consistent struggle for most companies. As technology continues to advance and Big Data analytics become more mainstream, organizations are generating enormous amounts of fresh data on a daily basis, more than any time since the creation of the Internet. To successfully manage, backup, and archive so much data, the levels of which cannot be successfully predicted in the years ahead, organizations need a scalable disaster recovery solution that is also efficient and cost-effective.

Today, the cloud offers improved data security, better reliability, and the greatest levels of efficiency, which also saves companies up to 50% of the costs associated with traditional recovery systems involving expensive hardware, physical storage space, and perhaps a secondary disaster recovery site. Here are twenty real-world business reasons to move to a cloud-based DRP.^[viii]

Disaster Recovery

1. Eliminate the need to replicate the organization's entire production system at a secondary, managed data center in another off-property location.
2. Replicated virtual machines can be used to access the recovery data from any global location.
3. By utilizing replicated virtual machines off-site, organizations can reduce IT downtime from days to minutes, resulting in a DRP with increased productivity and efficiency.
4. Cloud-based systems allow companies to replicate data in multiple locations within the cloud easily and cost-effectively while improving redundancy and boosting security simultaneously.

Backups and Restorations

5. Eliminate the need, dependence, administrative overhead, and other expenses associated with on-site hardware of a traditional DRP.
6. Companies pay for only what they use, scaling the services instantly to meet constantly evolving business requirements.
7. Cloud-based backup and restoration systems are more reliable, cost-effective, and faster while also allowing a multi-regional infrastructure that traditional systems simply cannot provide.
8. Data is fully encrypted, both at rest and in transit, while also being free from vendor access.

Archiving

9. Cloud-based systems streamline the archival process, lowering associated costs, reducing human error, and eliminating organizational dependence on fragile tapes and hardware.
10. Highly advanced deduplication technology provides more efficient and cost-efficient data storage over the long term.
11. Because the cloud is always easily accessible from any global location, data is always readily available for compliance issues, data mining, or perhaps legal disputes and concerns.

Testing and Development

12. Without the reliance on fixed and dedicated hardware, testing and development can occur at any time and from any location.
13. By locating a copy of all virtual machines, programs, and data in the cloud, testing can be run as needed without jeopardizing essential in-house production environments.
14. A centrally managed virtual machine can be replicated across different geographical locations for 24/7 testing, development, and management.
15. Eliminate the need for multiple testing and development systems by repurposing virtual machines.

Converged Architecture

16. Converge multiple workloads into a “single pane of glass” with the assurance that cloud-stored data adheres to global data privacy regulations.
17. Because a cloud-based Disaster Recovery Program relies on a single data source, organizations eliminate redundancies and save money on other corporate resources.
18. Companies can turn on and off individual services easily and instantaneously.

Data Analytics

19. A cloud-based data recovery model increases visibility and accessibility to existing data, which allows the organization to manipulate and leverage the data more easily to provide additional business value.
20. Organizations can analyze backed up data more effectively to understand more clearly the challenges and risks related to storage growth, dormant data, and data classification.

Potential Obstacles for a Successful Transition

One of the biggest obstacles preventing some organizations from embracing a cloud-based DRP is the lack of experience and knowledge related to the different technologies to achieve cloud resilience across dispersed environments. Many companies have difficulty in determining which applications and data might have the greatest potential for cloud resilience, which sometimes makes these organizations rather reluctant to implement a new process. They might assume that additional IT, business, and recovery education is required before they can even begin a transition to the cloud. Furthermore, the key decision makers may not have an in-depth understanding of their current disaster recovery strategies.

Other companies may not possess the capabilities to automate different hardware restorations. If the brands and types of servers that the organization uses are physically or virtually dissimilar, then decision makers may fear that disparities in recovery efficiency will occur. Another common obstacle is that many companies utilize applications that cannot operate in a cloud environment, either because the vendor doesn't support them or because the program is a legacy application created in-house well before "The Cloud" came into existence.

Additional obstacles might include:

- Security concerns
- Compliance concerns
- Network latency and bandwidth concerns
- Cost concerns
- Scheduling concerns regarding the transition time and date
- Control issues related to cloud-based systems
- Perceptions that reliable and trusted vendors offering this service do not exist
- Concerns over possible lack of employee or upper management buy-in to a new cloud-based backup and recovery system

Choosing the Right Cloud-based Solution

Whether an organization has concerns regarding internal processes, such as technology constraints, business continuity preferences, costs associated with the transition and monthly service, or external pressures like regulatory demands, choosing the right type of cloud resilience solution, or perhaps a combination of types, is essential. Depending on the company's needs, the organization has three basic types of cloud solutions available:

1. Private Clouds

Commonly used for in-house management of the DRP, the organization creates a separate, scalable, virtualized cloud environment for backup and recovery of traditional data and application requirements across multiple service tiers.

2. Public Clouds

The business subscribes with a cloud service provider, allowing for a “pay-as-you-go” option. Rates are determined based on resiliency requirements for specific services, which can be added or deleted at any time.

3. Hybrid Clouds

The organization combines both private and public cloud services to design and implement a disaster relief strategy that perfectly fits the needs of the business, providing ultimate flexibility, agility, and risk tolerance for highly sensitive data and applications.

Transitioning to a Cloud-based Disaster Recovery Plan: Step by Step

Transitioning to a cloud-based DRP is not a difficult process, but it requires an orderly, pre-planned approach. Before the transition begins, detailed objectives regarding the DRP's design, implementation, and ongoing evaluation must be clearly identified. The transition should consist of four distinct stages: strategy, design, testing, and transformation.

Stage 1: Strategy

An end-to-end business continuity cloud strategy includes recovery and backup, data and system availability, and data archiving. Separately or combined, these services can help organizations use security-rich cloud technologies to recover from disruptions more quickly and cost effectively. The key considerations in strategizing the transition include:

- Understand the business direction and strategic objectives.
- Review existing business continuity requirements and objectives.
- Modify those that are no longer relevant or may require adaptation to a cloud-based DRP.
- Document the new business continuity requirements.
- Evaluate workloads to determine which data and software applications have the greatest potential for an easy transition to cloud recovery, either public or private. For some organizations, it may not make sense to transition the recovery needs of some data and applications to a cloud-based environment of any kind, neither public nor private.
- Select the most appropriate cloud delivery model.
- Before defining the cloud architecture, evaluate any potential network latency issues.
- Identify which legacy continuity processes that may need to change, including internal policies, procedures, training requirements, and communication protocols.
- Define timelines and milestones for the remaining stages.

Stage 2: Design

The purpose of the design phase is to generate a plan for the easiest implementation of the various business continuity tiers. Key considerations might include security, data latency tolerance, network bandwidth optimization, and testing requirements.

- Check with the organization's current Internet provider to determine the monthly usage cap, if applicable. Will additional charges result from the increased bandwidth required for cloud-based backups?
- Is the organization's current bandwidth capability sufficient to back up to the cloud in a timely, efficient, and cost-effective manner? Or is additional bandwidth needed?
- Consider the potential effects that the increased bandwidth usage may have on your day-to-day operations.
- Evaluate the technological requirements for different application-specific SLAs.
- Determine the best method for copying existing data and applications from on-premises to cloud-based resources.
- Consider the "Big Picture." How will the new cloud-based Disaster Recovery Plan integrate with your existing DRP? Which traditional processes need to be preserved?
- Update internal policies, procedures, training requirements, and communication protocols as required.
- Define the ongoing testing of the cloud-based DRP. How often will the new system be tested? What criteria defines a successful DRP test?

Stage 3: Testing

It is never a good idea to make any sort of transition without first conducting a thorough testing. This allows the organization to identify and resolve possible glitches in the transitional protocol.

- Select a small combination of data elements or applications to be transitioned or replicated to the cloud as a pilot program.
- Gather together those staff members who will ultimately be involved with the management of the new cloud-based DRP.
- Educate all team members of the proper procedures of the new cloud-based environment.
- Conduct the pilot program.
- Evaluate the process. What changes need to be made?
- Make any necessary adjustments.
- After making the modifications, conduct the pilot program again and re-evaluate.

Stage 4: Transformation

Testing can be repeated until the results are satisfactory. While it is important to resolve all of the possible glitches before making the final transition, testing is a wonderful way to allow the staff to gain confidence in the new system. Once the testing is complete, it is time to begin the final transformation to a new cloud-based DRP. Once it is in place:

- The in-house team supporting the transformation should help manage the organization's environment remotely, especially during the final stage of the transition.
- Tracking key performance indexes (KPIs) allows the company to optimize system response time or other performance attributes.
- The storage capacities, servers, network architecture, and productivity are tweaked to their full potential.
- Testing is a critical component of the transformation phase. Conduct another test to determine if the cloud-based solution successfully integrates with the existing DRP elements from the previous model.

Cloud-based Disaster Recovery for Improved Control

Disaster recovery plans have traditionally been viewed as an insurance policy that organizations hope never to use. In contrast, a cloud-based DRP can actually increase the company's ability to provide service continuity for key business applications. Since the cloud-based services can be accessed through a web portal, IT administrators can take advantage of a dashboard view to their organization's infrastructure.

For example, administrators can access the portal via the Internet to identify which servers need to be protected and replicated. Once the environment is defined through the portal, they can then generate reports and conduct other administrative tasks. While this administrative portal view is valuable, it is critical to evaluate cloud-based business continuity services to help ensure that the portal is not merely an administrative configuration tool but that it also provides the opportunity to initiate a failover and failback in real time.

In doing so, the administrator may reduce future occurrences of "declaring a disaster." Without the need for a formal declaration while possessing the ability to fail over from the portal, IT administrators gain much more control and can be significantly more responsive to the more mundane power interruptions that traditionally lead to a full deployment of the DRP.

Ongoing Refinement of Disaster Recovery Plans

A common challenge facing many traditional disaster recovery plans is the lack of certainty that the system will work when the time comes. On average, organizations only test their failover and recovery about twice per year, which is hardly adequate given the fact that technology is advancing at such a rapid pace. This lost sense of control causes many organizations to bring disaster recovery "in-house," which only diverts critical IT focus from more important functions, such as mainline application development.

Cloud-based business continuity provides the opportunity for more control and more frequent and testing of disaster recovery plans, even at the application or server level. And the tests can be conducted on the entire system or perhaps only a single application. For example, a critical e-commerce website application can be tested in the days preceding a huge Cyber Monday sale. Or an architectural firm can test a new version upgrade of their computer-aided design software to ensure that it integrates seamlessly with other programs before releasing the upgrade to engineering staff located in twenty regional offices around the globe. Implementing cloud-based DPRs is not only useful for overcoming disasters more quickly and cost-effectively. They can also be highly beneficial in preventing disasters from occurring in the first place.

Mixed Environments and Cloud-based Disaster Recovery

The notion of a “server image” is a critical component of any disaster recovery solution. As the complexity of IT departments continues to increase, including perhaps multiple server farms with possibly different operating systems, the ability to respond to a disaster also becomes more complex as a result. Enterprises are sometimes forced to recover using different hardware, which can take longer and increase the possibility of data loss and human error.

Today, many companies are implementing virtualization technologies in their data centers to help eliminate much of the underlying complexity while simultaneously optimizing infrastructure utilization. Meanwhile, the number of virtual machines being installed in company offices is growing exponentially in the past several years. According to a recent [Intel study](#), 98% of those surveyed either had plans to implement virtualization within the next 12 months or had already implemented it. [ix](#) As a result of this current trend, cloud-based business continuity solutions now offer both virtual-to-virtual (V2V) and physical-to-virtual (P2V) recovery to support these types of mixed environments.

CASE STUDY

The Royal Bank of Scotland: A Disaster with Global Ramifications

Many companies underestimate the importance of an easy-to-implement disaster recovery plan. They mistakenly assume that the only people who suffer from such an event are those inside the related organization. They fail to consider how the disruption will affect customers, clients, subcontractors, or perhaps the government agencies to which they report.

In 2012, the Royal Bank of Scotland (RBS) experienced an IT disaster that caused worldwide chaos. It was not a natural disaster from a hurricane or flood. The disaster occurred from a simple upgrade to a workload automation tool used to process the transactions of its customers. The automation tool was not to blame, but the internal processes that the RBS used to install the upgrade were faulty.

RBS administrators did not take the time to formulate a step-by-step plan for upgrading the software. They had no back-out plan in place, in case something went wrong midway through the upgrade, and they also did not have an effective and current DRP. Upon initiating the upgrade installation, the batch processing tool virtually shut down completely, remaining totally inoperable for several days. The result was a catastrophe of epic proportions that affected nearly every nation on the planet, a disaster that had never been seen before or since in the global financial sector.

The Immediate Impacts

Without the RBS batch processing tool, the documenting of all banking transactions instantly and abruptly ceased, including money withdrawals, deposits, transfers, and hundreds of other standard services that any reputable banking institution is expected to provide. With each passing minute, more and more transactions were not being documented and calculated, and eventually the entire IT infrastructure had to be taken offline, leading to even more severe problems:

- Customers of the RBS could no longer use their ATM cards, either for cash withdrawals or payment of goods and services.
- Checks could not be cashed or written.
- Bank-provided credit cards were instantly declined, regardless of the user's balance level or pre-defined line of credit.
- Automated transactions did not occur for its customers, including those for mortgage payments, car loans, and medical bills.
- Customers in the midst of purchasing a new home found themselves without the ability to pay the standard down payment or to even buy the home outright.

- People traveling outside of their hometown were instantly stuck in a strange town without the resources to get home, pay for a hotel room, or even buy gas for the car.
- One family was almost denied life support from a [Mexican hospital](#) for their young daughter. x
- Mothers were caught in grocery lines without the funds to buy diapers or formula for their young infants.
- After a particularly raucous night on the town, one unfortunate man was forced to spend the night in jail because no one in his family could access bail money.

The upgrade began on a Tuesday, June 19, 2012, and the resulting downtime lasted for several days. By the following Monday, the RBS issued a statement that all systems were fully operational, but they were mistaken. Accounting glitches were still occurring well beyond July 2 when some customers were still unable to withdraw cash. With no DRP in place, bank officials were forced to develop a more creative, costly, and highly inefficient solution.

Banking executives were forced to keep over 1,200 local branches open for 24-hours a day for several weeks. They even stayed open on Saturdays and Sundays, which had never happened before in a European nation. Employees were paid huge sums of money in overtime, and tellers were working two to a transition window. Temporary employees were hired in large quantities, and even the bank executives were working the floor, trying to manage the barrage of customer complaints and insults hurled in every direction.

The Long Term Aftermath

By the end of 2012, the RBS estimated a loss of \$194 million as a direct result of what should have been a simple software upgrade. However, more fines and penalties were still to come because the financial disaster affected banks in multiple other nations around the world. In fact, by the end of 2014, the RBS was fined another \$86 million for the global panic that ensued. Their brand name reputation has never fully recovered.

PUTTING IT ALL TOGETHER

The Royal Bank of Scotland is the perfect example of how a simple software upgrade can lead to devastating consequences. Having an effective Disaster Recovery Plan in place that is easy to implement and manage is crucial to any organization. However, organizations must realize that disaster recovery planning is not something to be taken lightly. It requires attention to detail, thorough and consistent testing, and a dedication focus on security of sensitive data and applications.

Whether choosing a private cloud, public cloud, or hybrid cloud combination, organizations that follow a cohesive multi-stage process of transition tend to achieve the highest rates of success. A cloud-based Disaster Recovery Plan that is cost-effective, infinitely scalable, and security-rich can provide organizations with the opportunity to improve their business continuity and resilience significantly while gaining full value from the associated low financial investment. Cloud computing offers a remarkable opportunity to combine the positive features of quick recovery times from dedicated disaster recovery models with the low-cost appeal of shared infrastructures.

FREE THIRTY MINUTE CONSULTATION

Bryghtpath has designed and implemented the business continuity & disaster recovery strategies used today by organizations ranging from small businesses, to global Fortune 30 corporations, and major law enforcement agencies.

We're happy to have a thirty-minute consultation with you and your team completely free – there is zero obligation to you following our discussion.

We guarantee you'll leave with some ideas about how to move forward and improve your business continuity and disaster recovery strategies.

To get started, visit us at bryghtpath.com/freeconsult or give us a call at +1.612.235.6435.

REFERENCES

- ^[i] Aberdeen Group, *Datacenter Downtime: How Much Does It Really Cost?*, March 2012,
- ^[ii] *The 2012 IBM Global Reputational Risk and IT Study survey*, conducted by the Economist Intelligence Unit, September 2012, RLW03009-USEN-00
- ^[iii] Forrester/Disaster Recovery Journal, *The State of Business Continuity Preparedness*, Winter 2012
- ^[iv] Neverfail, *Common Disaster Recovery Plan Misconceptions*, February 2013
- ^[v] Sullivan, Patricia (2012, July 11). *911 failure affected 2.3 million in Northern Virginia*. The Washington Post. Retrieved from <https://www.washingtonpost.com>
- ^[vi] Semantec, *2015 Internet Security Report*, April 2015
- ^[vii] Columbus, Louis (2015, January 24). *Roundup of Cloud Computing Forecasts and Market Estimates, 2015*. Forbes Magazine. Retrieved from <http://www.forbes.com>
- ^[viii] Packer, Dave (2016, February 2). *20 Reasons to Move Backup and Disaster Recovery to the Cloud*. Druva. Retrieved from <http://www.druva.com>
- ^[ix] Intel, *Peer Research: Cloud Computing Research for IT Strategic Planning*, January 2012
- ^[x] Bains, Inderdeep (2012, June 24). *Family's fears cancer girl could die in Mexico after NatWest computer glitch meant crucial funds could not be transferred*. The Daily Mail. Retrieved from <http://www.dailymail.co.uk>

ACKNOWLEDGEMENTS

Bryghtpath LLC wishes to recognize the contributions of many business continuity, disaster recovery, and information technology professionals in the Minneapolis – Saint Paul, Minnesota (USA) area that contributed to this white paper through their feedback, comments, proofreading, and edits.

ABOUT THE AUTHOR

BRYAN STRAWSER, CEO, BRYGHTPATH LLC
@BRYANSTRAWSER

Bryan Strawser is a globally recognized strategist and thought leader who founded Bryghtpath LLC in 2014 after a 21-year career at Target Corporation where he built and led the retailer's Global Crisis Management and Business Continuity function. Under his leadership, Target received numerous awards from the Federal Emergency Management Agency (FEMA), the International Association of Emergency Managers (IAEM), and the Business Continuity Institute (BCI).

A valued industry leader, Bryan previously served as a board member and Chair of the Private Sector Committee for the National Emergency Management Association (2011 – 2013) and as the Vice Chairman of the Retail Industry Leader's Association's Disaster Recovery and Preparedness Committee. In these roles, Bryan worked closely with FEMA to develop the Private Sector Representative position in FEMA's Office of the Private Sector and with leaders across state and federal government, including the US Department of Homeland Security and the White House, to build stronger connections between the public and private sectors.



Bryan holds multiple professional certifications in business continuity, emergency management, information security, project management, and physical security.

He is a member of the International Association of Professional Security Consultants, the Private Sector Committee of the National Emergency Management Association, and the Royal Institute of International Affairs (Chatham House, London).

Bryan holds a Bachelor of Science in Criminal Justice Administration from the University of Phoenix and a Master's in Business Administration (MBA) from the University of Minnesota's Carlson School of Management. He is a graduate of the National Preparedness Leadership Initiative Program at Harvard University's School of Government.

CONTACTING BRYAN

Bryan.Strawser@bryghtpath.com
+1-612-235-6435

ABOUT BRYGHTPATH LLC

Bryghtpath LLC is a strategic advisory firm that specializes in global risk, business continuity, emergency/crisis management, crisis communications, and public affairs.

Our team of globally recognized experts offer strategic counsel on identifying, preparing for, and managing risk to your company, non-profit, or public sector agency.

Bryghtpath works with the world's leading brands, public sector agencies, and nonprofits to develop strategies to help them strategically navigate global uncertainty.

OUR PRACTICE AREAS

- Business Continuity / Continuity of Operations
- Crisis / Emergency Management
- Crisis Communications
- Emergency Planning & Exercises
- Intelligence & Global Security Strategies
- Speaking / Training

LEARN MORE

- Our services: bryghtpath.com/services
- Case studies & results: bryghtpath.com/results

LET'S CONNECT

We're always happy to provide examples of our work, free proposals, or to talk through any services that you may need. All of our services are customized for your specific needs.

+1.612.235.6435 | contact@bryghtpath.com | bryghtpath.com