COMMVAULT®

▶ Balancing Cost, Risk and Complexity in Your DR Strategy

In the face of more frequent disaster situations and a higher reliance on technology, disaster recovery (DR) and business continuity have become absolutely vital for maintaining an edge in today's competitive business environment. Successful companies embrace a multi-tiered catalog of recovery technologies connected by a unified management platform. This approach enables IT departments to continuously balance cost vs. risk, leverage the cloud for DR, and protect data accordingly.

Building a solid tiered DR catalog is challenging for most organizations. Companies often rely on third-party consultants and technical experts to help them transform their legacy IT approaches to realize the most value. Disaster recovery should be no exception. This paper outlines key considerations for balancing cost, risk and complexity when implementing a comprehensive DR strategy and provides guidance on how to realize a pragmatic future state.

▶ Contents

THE FACE OF DISASTER RECOVERY IS CHANGING

Disaster management and business continuity activities are absolutely vital for maintaining an edge in today's competitive business environment. Even our largest cities must deal with the effects of hurricanes, floods, fires and earthquakes. In northeastern Japan the Tohoku earthquake had devastating consequences on its people and infrastructure in 2011. The 9.0 magnitude earthquake and ensuing tsunami left over 900,000 buildings damaged and interrupted operations for many large Japan based corporations. The most recent, high profile disaster in the US, Hurricane Sandy, impacted the American financial district and affected more than 25% of the US population to varying degrees and brought large parts of the New York City area to a standstill.

Since the 1950s, the Federal Emergency Management Agency (FEMA) has tracked disaster declarations and relief requests. The data shown in Figure 1 makes it clear that the long-term trend for major disaster declarations is on the rise. In the 1950s, disaster declarations numbered in the teens annually. During the 1970s, the annual US disasters ranged in the low 30s. During the past decade, declarations peaked in 2011 with 99 declared disasters.[1]
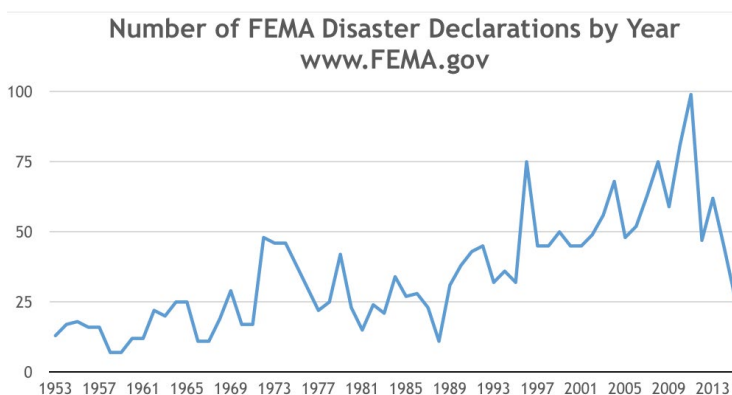

Figure 1 – FEMA Disaster Declarations

There are many reasons for this spike in disaster declarations; one of which is undoubtedly the growing sensitivity we have towards the impact of environmental factors on our national infrastructure. Computer technology has become a critical component for the way businesses manage their supply chain, market and sell to customers, and even how they communicate with investors. Growth and globalization, along with a fundamental reliance on computer technologies, have enhanced our lives and improved business efficiency. This reliance also means the cost of a disaster is higher than it has ever been.

TIME TO GET SERIOUS ABOUT DISASTER RECOVERY

As companies become more dependent on technology to conduct even simple business tasks, it's clear that protecting against disaster is vital for business success over the long haul. Disaster recovery planning and design

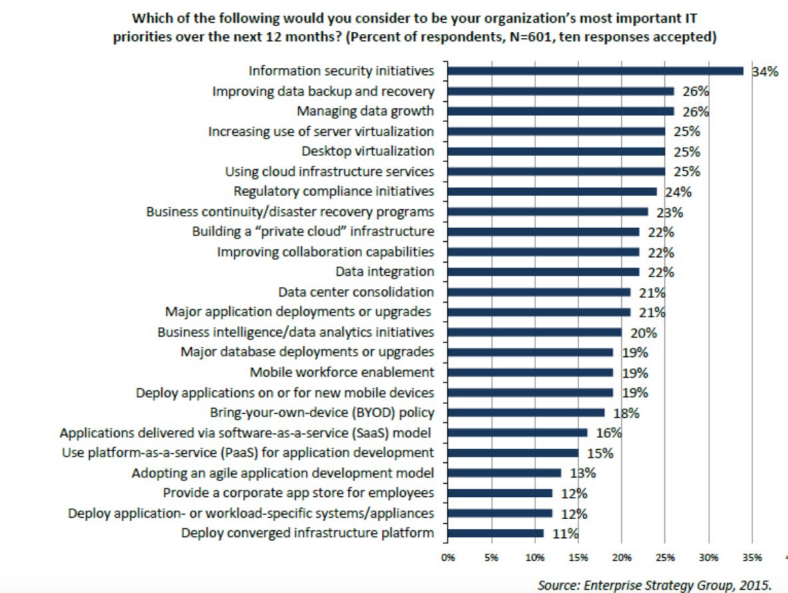1 Federal Emergency Management Agency, http://www.fema.gov/Disasters

are necessary activities that, if overlooked, will place your company in a very uncomfortable position. Imagine explaining to thousands of customers why you're not open, when your competitor across the street has actually extended hours. How would you tell your key suppliers that deliveries will not be needed or that payments will be delayed? Will your shareholders be sympathetic to a material impact on revenue and profits resulting from poor disaster planning?

Then there are the costs related to downtime. In fact, IDC research indicates that the average cost of downtime is about $100,000 per hour, although it can go as high as $1.6 million per hour for some organizations. IDC also found that most organizations experienced between 10 and 20 hours of unplanned downtime per year, even without a disaster.[2]

Yet, even with the high cost of downtime, there is still, according to Gartner,[3] "an imbalance in the investments made in DR by infrastructure and operations leaders including money, thought and effort expended." This, Gartner says, "results in less protection or excessive diversion of resources needed in other areas of the business."

The challenge grows with the influx of big data. Enterprise Strategy Group (ESG) points out that "with big data finally becoming mainstream and adoption growing in global enterprises in all industries, the requirements for resilience and robustness of the applications have increased."[4] This drives an increasing need to look a disaster recovery more strategically with modern approaches that will drive better reliability and business continuity.

Fortunately, businesses are taking notice and not taking chances. In another recent ESG study,[5] improving data backup and recovery was a top IT priority for 2015 coming in second only to information security initiatives.

Which of the following would you consider to be your organization's most important IT priorities over the next 12 months? (Percent of respondents, N=601, ten responses accepted)

Information security initiatives	34%
Improving data backup and recovery	26%
Managing data growth	26%
Increasing use of server virtualization	25%
Desktop virtualization	25%
Using cloud infrastructure services	25%
Regulatory compliance initiatives	24%
Business continuity/disaster recovery programs	23%
Building a "private cloud" infrastructure	22%
Improving collaboration capabilities	22%
Data integration	22%
Data center consolidation	21%
Major application deployments or upgrades	21%
Business intelligence/data analytics initiatives	20%
Major database deployments or upgrades	19%
Mobile workforce enablement	19%
Deploy applications on or for new mobile devices	19%
Bring-your-own-device (BYOD) policy	18%
Applications delivered via software-as-a-service (SaaS) model	16%
Use platform-as-a-service (PaaS) for application development	15%
Adopting an agile application development model	13%
Provide a corporate app store for employees	12%
Deploy application- or workload-specific systems/appliances	12%
Deploy converged infrastructure platform	11%

Source: Enterprise Strategy Group, 2015.

2 IDC, "Leveraging the Public Cloud for Faster Disaster Recovery at Lower Cost," May 2015
3 Gartner, "Prioritize Disaster Recovery Investments to Maximize Business Value," December 2014
4 Enterprise Strategy Group, "ESG Brief: Data Protection and Disaster Recovery for Big Data," April 2014
5 Enterprise Strategy Group, "2015 IT Spending Intentions Survey," February 2015

ISN'T DISASTER RECOVERY PROTECTION EXPENSIVE?

Traditionally, the installation, operation, and maintenance of comprehensive Disaster Recovery capabilities have been perceived to be cost prohibitive. CEOs and CFOs are usually reluctant to spend large portions of their IT budget on "protection" measures. Let's face facts, the technology spending climate does not support large budgets for something that executives hope they will never use. This cost-directed approach to Disaster Recovery drives organizations to either protect everything by using their existing backup environment, expecting it to be the cheapest solution, or they provide a high cost solution for only a select few applications. Here are two examples of how these approaches can steer planners down the wrong path:

1 On the cheap – Tape backup is often carried out nightly and tapes sent to offsite storage the next morning. In the event of a disaster, these tapes are rushed to a recovery location so the restore process can begin. This approach seems economical on the surface, but doesn't scale well. It can be extremely difficult to test recovery fidelity and requires significant resources, often yielding a slow recovery time (RTO). Furthermore, a disaster event at the time of the daily tape shipment will mean that tapes from the previous day have to be used, increasing data loss to upwards of 36 hours (RPO) or more.

2 Spare no expense – An alternative to slow tape-based recovery is array or application-based replication, which can deliver fast recovery. Replication is used to create synchronous or asynchronous copies of key application data at an offsite location. This approach allows you to achieve very low levels of data loss (RPO) in the event of a disaster and facilitates fast recovery time (RTO). It however can be extremely expensive to implement and maintain. It also requires additional protection strategies for operational data loss or corruption; so standard backup is still needed. From a cost perspective this option may not be a strong fit for many data types.

For those who take the "cheap" approach, the total cost of managing offsite tape copies isn't as cheap as they might expect. As data grows, so does the cost to maintain offsite copies. Tape handling, media, rotation, storage, and transportation all add up. Taken in aggregate, this often leads to a recovery environment that is too complex to test and too difficult to recover reliably in the event of a disaster. It's also typical that given the higher amount of data loss associated with recovery from tape, concessions have to be made causing DR capabilities to be misaligned with business goals and needs.

Others who take the "spare no expense" approach often start by replicating data from a few key applications in order to keep costs down. But once the word gets around management circles, every Vice President demands this option for their applications, rather than accept the risk of

IDC Whitepaper: Leveraging the Public Cloud for Faster Disaster Recovery at Lower Cost[i]

Read how cloud computing can be leveraged to develop DR capabilities that are both less expensive and easier to deploy than traditional methodologies.

READ NOW

PDF

36 hours or more of data loss with traditional tape backup. For much of their data, the business needs a higher level of protection than tape that can't be cost justified for array based replication. What they really need is an affordable option that provides a higher level of protection than tape.

▶ POINT SOLUTIONS CREATE COMPLEXITY AND UNCERTAINTY

By not addressing your company's need to align risk and cost with business needs, your DR capability will eventually evolve into an unbalanced state. You may end up with a few applications using replication, but the majority of applications will default to tape-based backup because it's just too expensive to justify replication across your entire production environment. The large divide between replication-based DR and the lack of scalability of tape-based recovery, provides a breeding ground for one-off point solutions and departmental work-arounds. In this unbalanced state, it's nearly impossible to ensure that reliable recovery from a disaster is achievable. With a mix of sanctioned and unsanctioned DR technologies, the complexity of recovering increases dramatically. The result will be an unpredictable recovery capability at best, and most likely data loss in the event of a disaster.

▶ IT DOESN'T HAVE TO BE THIS WAY, REALLY!

Balancing cost against the time to recover (RTO) requires an in-depth understanding of your application's RTO/RPO requirements and the technologies needed to meet them. Given the advancements in network optimization, data compression, and data deduplication, the expectation that suitable DR has to be expensive is outdated. This is furthered by new developments in cloud-based DR architectures that can yield even more DR cost savings. These now ubiquitous technologies enable IT departments to build affordable alternatives to expensive replication schemes while providing large improvements in RTO and RPO over tape-based disaster recovery. The ultimate goal for nearly any business is to build a recovery service catalog with mid-tier options that scale with changing business needs.

The recovery catalog shown in Table 1 builds on the scenarios described earlier and includes two generally accepted approaches for affordable, scalable disaster recovery. These recovery tiers can easily be implemented in the cloud to minimize the need for acquiring target recovery assets and datacenter space, as well as provide a "pay for use" DR procurement strategy. This can be especially valuable for corporate assets that are remote and beyond the reach of a traditional hub and spoke approach.

The average cost of downtime is about $100,000 per hour, although it can go as high as $1.6 million per hour for some organizations.

IDC
"Leveraging the Public Cloud for Faster Disaster Recovery at Lower Cost," May 2015

Cost vs. Risk Alignment

Scalable Middle Tiers

	Tier 1	Tier 2	Tier 3	Tier 4
Example Technology	Sync/Async, CDR, Application, Replication	LiveSync, Replicated Snapshots	Disk-Based Backups	Restores from Tape
Application Business Criticality	Business Critical Applications	Business Sensitive Applications	Business Sensitive Applications	Non-Critical Applications
Disaster RPO	0-15 Minutes	Snap Freq based 4-24hrs	Backup frequency based 6-24 hours	36 hours
Disaster RTO	Less than 4 hours	12-72 hours	12-72 hours	Best Effort
Relative Costs	$$$$	$$$	$$	Many Hidden Costs

Table 1- Representative Recovery Catalog

> **Tier 1**- Synchronous, asynchronous, and application replication will remain among the most aggressive RPO/RTO capable solutions. This option still requires traditional backup for day-to-day recovery purposes.
>
> **Tier 2**- Near continuous and replicated snapshots provide a cost effective alternative to sync/async replication, with relatively low recovery time and minimal data loss. Snapshots can also provide operational recovery capabilities that can integrate with backup processes.
>
> **Tier 3**- Replicated, deduplicated, disk base backups (DASH Copies) are typically lower cost than technologies in Tier 2, yet can provide the most flexibility and value. This approach can be used for DR between core datacenters as well as for edge-to-core, remote-site-to-core protection, as well as DR to the cloud.
>
> **Tier 4**- Tape based backup may be slow to disappear. It still may have a legitimate place in your data protection scheme. However, consider the potential hidden costs and scalability issues compared to alternatives.

ELASTIC IS FANTASTIC

The primary benefit of building a Recovery Service Catalog like the one shown in Table 1 is that the middle recovery tiers are elastic; readily scaling up or down for better cost and capacity alignment. The key enabler of elasticity is the management platform used across recovery tiers. The management platform must unify the tiers, or much of the value of tiering will be lost. Islands of disparate technology become an operational obstacle to maintaining and managing DR. This operational efficiency is typically where large cost savings are realized. In order to create more operational efficiency, you need a robust data management platform that unifies as many recovery tiers as possible. The ultimate goal is to have the flexibility to move existing applications and their

associated data between tiers of recovery, through a common interface and single point of data protection policy management, as business needs for recovery change. This management layer should also allow you to automate DR management tasks, track and report on recoverability, and build comprehensive DR test workflows to further drive down operational costs. Many traditional management tools in place today do not provide that flexibility to change with business needs. Unfortunately, they deliver a fragmented solution and tend to foster a siloed DR environment.

Cloud has become an increasingly important part of Disaster Recovery testing. This is especially relevant for DR testing using the public cloud. When a test is complete, resources in the public cloud can be shut down, allowing companies to eliminate charges for infrastructure that would normally continue for years. Furthermore, these cloud based DR test assets can be updated regularly, in accordance with corporate policy for RPO, and provide confidence that in the event of a disaster declaration, they can be brought into production using the cloud.

Another facet of elasticity enabled by a unified management platform is that it allows you to optimize cost and risk among your DR tiers. In the past, many have taken a "set it and forget it" approach to DR service provisioning. It is imperative that Disaster Recovery is regularly tested, and business needs are re-evaluated regularly so that tiers and resources can be adjusted to maintain business alignment. An appropriate, unified management platform facilitates re-alignment by providing visibility across the data protection environment, as well as seamless movement of your application data between recovery tiers.

SIMPLIFY FOR SUCCESS

Building a sound DR capability draws from most areas of your IT infrastructure. Recovery from a disaster is similar to a forced migration of your entire data center. The most important aspect of conducting a successful migration is reducing complexity. The point here is that to develop a successful DR capability, much like with a migration, the technology that you employ to deliver your DR capability must reduce complexity in the recovery process. Here are some ways to reduce the complexity within your DR environment:

- Single management platform for recovery
- Embedded cloud DR functionality
- Pre-position data
- Remote management of recovery processes
- Automate DR workflows
- Align with a technology partner invested in your DR success

Don't Get Lost in the Clouds[ii]

Read about the key advantages the cloud can bring to your data protection processes and the barriers you need to consider to ensure that you are truly realizing the cloud's value.

READ NOW

PDF

► BUILDING A SOLID DISASTER RECOVERY STRATEGY

Now that you've found ways to balance costs, risks and complexity within your DR environment, you will need to strike a balance among each in order to build a successful DR capability. As business requirements shift, your DR strategy needs the flexibility to rebalance and grow with you. We've provided examples of how a tiered DR capability can drive down costs by reducing and potentially eliminating the complexity of tape based recovery. Other cost reductions are gained by providing viable options to array-based replication.

There are scalable middle tiers that can be used to scale out your DR capability, and all can leverage Cloud Data Protection. These solutions are widely available and support many open systems hardware combinations. Properly architecting these solutions and leveraging a unified management platform will better position you to deliver aligned Disaster Recovery capabilities that fit your business and technical requirements.

The cloud has become a valuable resource for retaining both cost efficiency and agility in your DR strategy. With each passing year both private and public cloud have become a critical piece of disaster recovery design. According to Forrester, backup and DR is the number three planned use case for the public cloud, and the number one planned use case for private cloud.[6] Gartner has also noted that by 2020 as many as 9 in 10 DR operations will run in the cloud and by 2016, one in two Global 1,000 companies will have customer-sensitive data stored in the public cloud.[7]

Beyond cloud-based options, it's also important to evaluate options that support a heterogeneous environment. This will give you the flexibility and freedom to choose the best technology options in the future, without vendor lock in or portability restrictions. As your business needs change and demand more scalability, your disaster recovery approach needs to be able to adapt easily to continue to deliver reliable and resilient protection.

Whether on premise, or in the cloud, each organization's requirements for disaster recovery is unique. Designing, developing, and implementing a tiered DR environment is not for every business. For some businesses, only one or two DR options are appropriate; however even for those environments, understanding the options and potential pitfalls is important for making the final decision on which technology and approach is right. There are many technologies in the data management space, which is constantly evolving. Understanding each technology's technical and operational benefits, and how they fit together to meet your needs, requires much investigation and comparison. It's important that you partner with a vendor that's interested in the whole DR picture and not just one piece of the puzzle.

By 2020 as many as 9 in 10 DR operations will run in the cloud and by 2016, one in two Global 1,000 companies will have customer-sensitive data stored in the public cloud.

GARTNER SYMPOSIUM
2014

---

6   Forrester Business Technographics global Infrastructure Survey, 2014
7   Gartner Symposium, 2014

Disaster Recovery is where Commvault Services excels. Our consulting and professional services organizations are experts at helping companies understand and define their DR needs, designing efficient and flexible DR capabilities, and working side-by-side with them to implement and manage a new DR infrastructure. Commvault consulting experts leverage their combined years of experience from thousands of similar client engagements to ensure exceptional customer experience and outcomes.

Our consultants serve as trusted advisors who partner with clients to understand their current environment, envision a pragmatic future state, and develop architectures and processes to realize their goals. We lead our customers on transformational journeys with proven, consultative methods and industry specialists in Modern Data Protection, Disaster Recovery, Archive and Compliance, and Operations Optimization. We help our clients to design, build, and operate the optimal modern data and information management environment for their business.

If you're interested in how Commvault can help you transform your Disaster Recovery capability, visit Commvault.com or email ConsultingServices@commvault.com to start a conversation and discover what the Commvault Consulting Services team can do for you.

▶ ## RESOURCES

i commvault.com/resource-library/555d8b0d00e072a74700007f/idc-report-leveraging-the-public-cloud-for-faster-disaster-recovery-at-lower cost.pdf%20

ii commvault.com/resource-library/5522b12cea866914000001e5/dont-get-lost-in-the-clouds.pdf

▶ To learn more about how Commvault will enable cloud-enabled data protection, visit **commvault.com/cloud**.

COMMVAULT®

▶ PROTECT. ACCESS. COMPLY. SHARE.

COMMVAULT.COM | 888.746.3849 | GET-INFO@COMMVAULT.COM
© 2015 COMMVAULT SYSTEMS, INC. ALL RIGHTS RESERVED.