

BALANCING COST, RISK AND COMPLEXITY IN YOUR DR STRATEGY

James Brissenden: CommVault Services Development Manager

Jeff Dorr: CommVault Marketing Manager

Abstract: In the face of more frequent disaster situations and a higher reliance on technology, Disaster Recovery 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 and protect data accordingly.

Building a solid tiered Disaster Recovery catalog organically is challenging for most organizations. Companies often rely on third-party consultants and technical experts to help them transform their legacy IT approaches. Disaster Recovery should be no exception. CommVault 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.

Contents

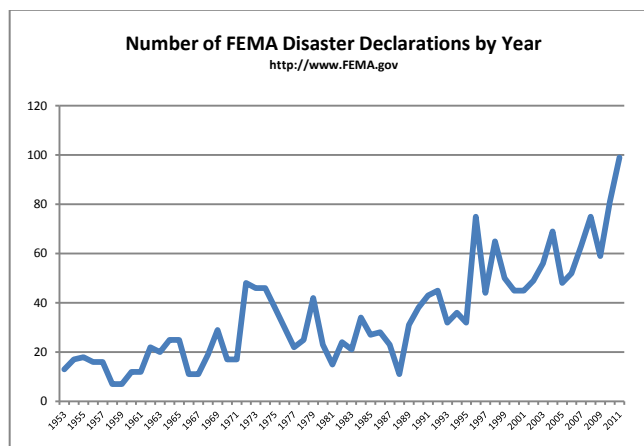
The Face of Disaster Recovery is Changing	3
Time to Get Serious About Disaster Recovery	3
Isn't Disaster Recovery Protection Expensive?	5
Point Solutions Create Complexity and Uncertainty	6
It Doesn't Have To Be This Way, Really!	7
Elastic is Fantastic	8
Simplify for Success	9
Building a Solid Disaster Recovery Strategy	9
About CommVault.....	10

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 number of 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 have spiked to an average of 56 per year and peaked in 2011 with 99 declared disasters.

Figure 1 – FEMA Disaster Declarations



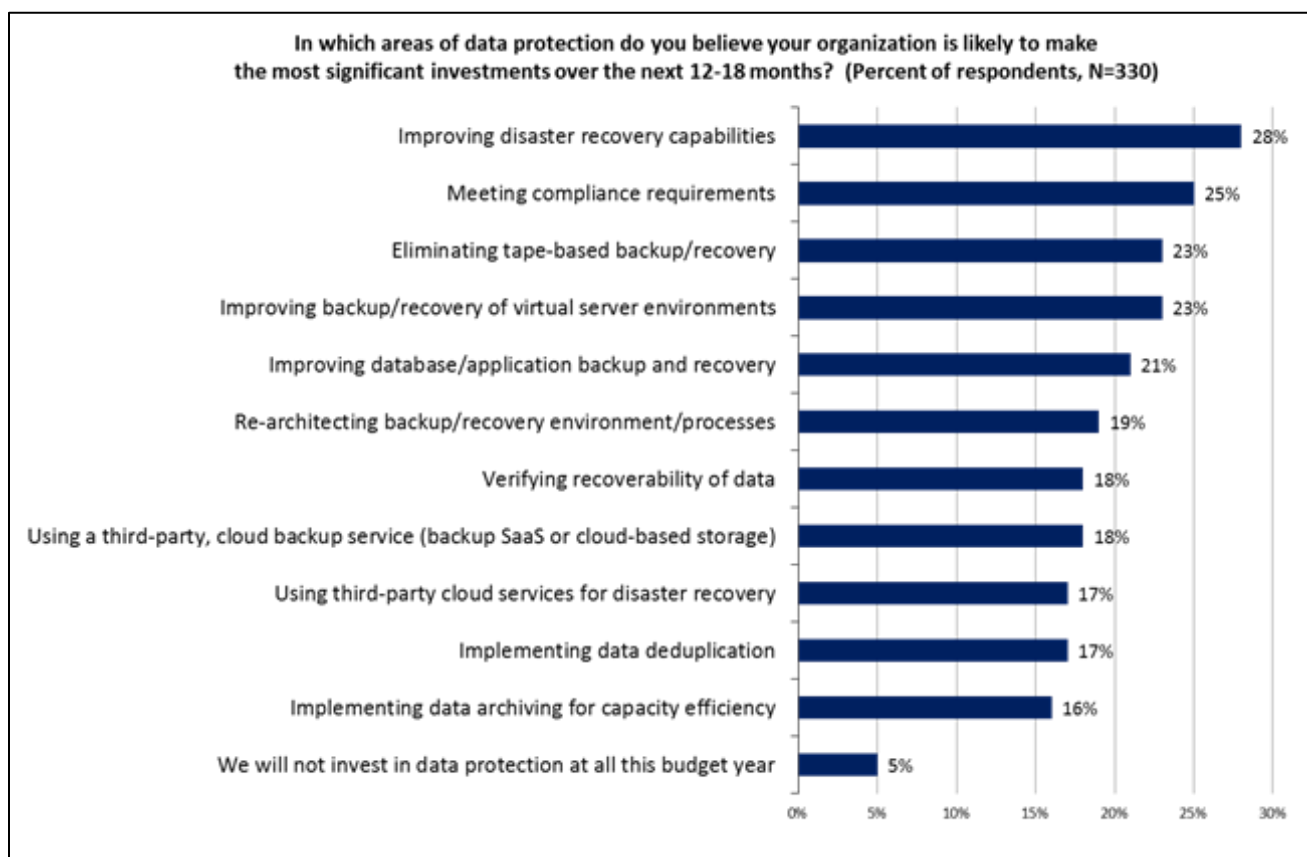
There are many reasons for this spike in disaster declarations; one of which is undoubtedly the growing sensitivity we have towards the impact of environmental factors on our national infrastructure. Computer technology has become a critical component for the way businesses manage their supply chain, 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 is clear that protecting against disaster is vital for business success over the long haul. Disaster recovery planning and design 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?

Fortunately, businesses are taking notice and not taking chances. A recent study by researchers at the Enterprise Strategy Group (ESG) indicate that improving disaster recovery is the top data protection spending initiative for many companies during 2012-13.

Figure 2 – Top Areas of Data Protection Investment



Enterprise Strategy Group, The Modernization of Data Protection, Jason Buffington, April 2012

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:

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.

Spare no expense – An alternative to slow tape-based recovery is array-based replication, which delivers extremely fast recovery. This technology 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.

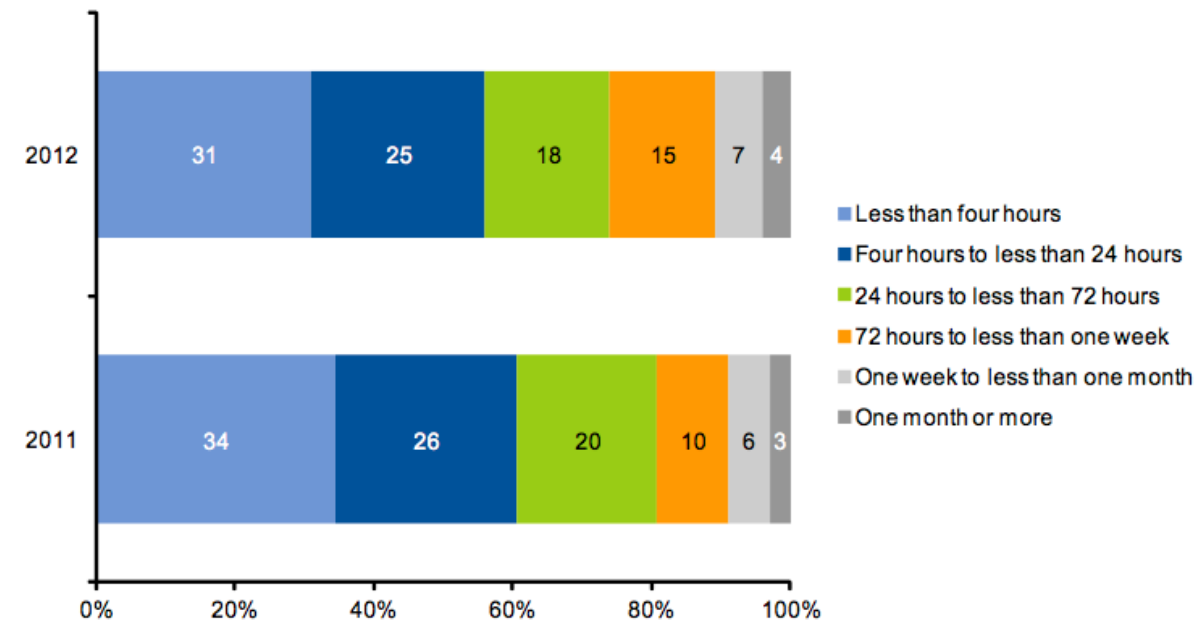
Others who take the “spare no expense” approach often start by replicating data from a few key applications in order to keep costs down. But once the word gets around management circles, every Vice President demands this option for their applications, rather than accept the risk of 36 hours or more of 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 is 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.

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. Research by Gartner shown in Figure 3 provides insight into the RTO for 156 of their customers. In a recent study in 2012, Gartner found that 31 percent of respondent environments required a recovery time of less than 4 hours. Twenty-five percent of their environment required between 4 and 24 hour recovery. With 18 percent falling between 24 and 72 hours, that means that 74 percent of their respondents’ environments needed to be restored within a 72 hour period. For a mid-size to large enterprise company, recovery from tape will never be able to scale to meet these high-volume, low RTO environments. As for array-based replication, the cost for replicating a large portion of your data just doesn’t seem economically feasible, does it?

Figure 3- Percentage for Recovery Time Objectives



Source: Gartner (July 2012)

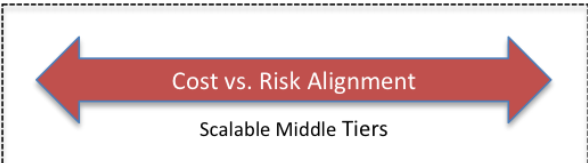
Gartner, *Survey Analysis: IT Disaster Recovery Management Spending and Testing Activities Expand in 2012*, John P Morency & Kevin Knox, July 18, 2012

It Doesn't Have To Be This Way, Really!

Given the advancements in network optimization, data compression, and data deduplication, the expectation that suitable DR has to be expensive is outdated. 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 to 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. It also includes an increasingly popular Cloud based option that offloads much of the operational DR burden. This can be especially valuable for corporate assets that are remote and beyond the reach of a traditional hub and spoke approach.

Table 1- Representative Recovery Catalog



	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5
Technology	Array-Based Replication	Cloud Data Protection & SaaS	Replicated Snapshots	DASH Copies	Restores from Tape
Application Business Criticality	Business Critical Applications	Business Sensitive Applications	Business Sensitive Applications	Business Sensitive Applications	Non-Critical Applications
Disaster RPO	0-15 Minutes	0-15 Minutes	Snap Freq based 4-24hrs	Backup frequency based 6-24 hours	36 hours
Disaster RTO	Less than 4 hours	Less than 4 hours	12-72 hours	12-72 hours	Best Effort
Relative Costs	\$\$\$\$	\$\$\$	\$\$\$	\$\$	Many hidden costs

Tier 1- Array-based replication will remain among the most aggressive RPO/RTO capable solutions, but at the highest cost. This option still requires traditional backup for day-to-day recovery purposes.

Tier 2- Cloud Data Protection and SaaS can be an extremely effective way to protect business sensitive applications from disaster and downtime. Storing and protecting key application data in the cloud allows you to decouple applications from IT infrastructure, geographical region, and the disasters that impact them. There are a number of criteria to consider when choosing a cloud vendor for DR. Key aspects include: resiliency and SLAs, recovery zones, cross border data transfer, and scalability.

Tier 3- Replicated snapshots provide a cost effective alternative to sync/async array based replication, with relatively low recovery time and minimal data loss. Snapshots can also provide operational recovery capabilities that can integrate with backup processes.

Tier 4- Replicated, deduplicated, disk base backups (DASH Copies) are typically lower cost than Tier 3, yet provide the most flexibility and value. This approach can be used for DR between core datacenters as well as for edge-to-core and remote-site-to-core protection.

Tier 5- 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; 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 is 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 silo'd DR environment.

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 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
- Pre-position data
- Remote management of recovery processes
- Automate DR workflows
- Align with a technology partner invested in your DR success

Building a Solid Disaster Recovery Strategy

We’ve discussed 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 three scalable middle tiers that can be used to scale out your DR capability, including: Cloud Data Protection, Replicated Snapshots, and backup to disk that is DASH copied offsite. 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.

Each situation is different. 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.

Disaster Recovery is where Simpana software and CommVault Services excel. Our consulting and professional services organizations are experts at helping companies 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.

About CommVault

A singular vision—a belief in a better way to address current and future data management needs—guides CommVault in the development of Singular Information Management® solutions for high-performance data protection, universal availability and simplified management of data on complex storage networks. CommVault's exclusive single-platform architecture gives companies unprecedented control over data growth, costs and risk. CommVault Simpana® software was designed to work together seamlessly from the ground up, sharing a single code and common function set, to deliver superlative backup and recovery, archive, replication, search and resource management capabilities. More companies every day join those who have discovered the unparalleled efficiency, performance, reliability, and control only CommVault can offer. Information about CommVault is available at www.commvault.com. CommVault's corporate headquarters is located in Oceanport, New Jersey, in the United States.



For more information about Simpana® software modules and solutions, and for up-to-date system requirements, please visit www.commvault.com

www.commvault.com • 888.746.3849 • info@commvault.com
CommVault Worldwide Headquarters • 2 Crescent Place • Oceanport, NJ 07757
Phone: 888.746.3849 • Fax: 732.870.4525

CommVault Regional Offices: United States • Europe • Middle East & Africa • Asia-Pacific • Latin America & Caribbean Canada • India • Oceania

©1999-2013 CommVault Systems, Inc. All rights reserved. CommVault, CommVault and logo, the "CV" logo, CommVault Systems, Solving Forward, SIM, Singular Information Management, Simpana, CommVault Galaxy, Unified Data Management, QiNetix, Quick Recovery, QR, CommNet, GridStor, Vault Tracker, InnerVault, QuickSnap, QSnap, Recovery Director, CommServe, CommCell, IntelliSnap, ROMS, Simpana OnePass, and CommValue, are trademarks or registered trademarks of CommVault Systems, Inc. All other third party brands, products, service names, trademarks, or registered service marks are the property of and used to identify the products or services of their respective owners. All specifications are subject to change without notice.