The CTE Group

White Paper

THE BEAT GOES ON

Why Data Protection Presents So Many Challenges

By: David A. Chapa, Sr. Analyst
The CTE Group

December, 2019

Contents

INTRODUCTION

When protecting your data, the beat really does go on. Data protection remains a challenge because the digital assets that we protect, and the governance surrounding these assets, continue to increase in complexity, requiring ever-higher degrees of operational efficiency in order to meet or exceed business and regulatory requirements. For IT to deliver at the speed of business, it must be fully equipped with the right software solutions, and with hardware and cloud solutions as well. This paper and its companion pieces cover the complexities that data protection presents and its effects on simple recovery and on disaster recovery, The papers also discuss NetApp’s approach to mitigating these ever-present data protection challenges.

BACKUP USED TO BE SO SIMPLE

If you've been in this industry for a long time, you might say that "back in the day, backup was pretty simple." In reality, looking back, we faced similar challenges to those we face today. I believe that as time passes we tend to forget some of the challenges we faced and reminisce about the "good old days" of data protection. We logged people out of applications, locked logins, backed up the data to tape, and kicked off a scheduled tape-to-tape copy for disaster recovery.

WHEN DID IT CHANGE?

It's hard to pinpoint exactly when it all changed; in fact, I believe that data protection evolved slowly over time with new regulations, different datasets, 7/24/365 operation, virtualization, and the cloud. However, we can pinpoint when new regulations started to change things for us in data protection. These regulations presented hurdles that IT had to overcome with their available tools.

For example, in 1996 HIPPA came into effect, followed by the Sarbanes-Oxley Act in 2002. These acts were designed to increase security for the consumer, but when they were introduced, the language around data protection requirements simply stated that we had to present an auditable data protection plan. Today, the language is much stricter and requires us to maintain a data protection process for assets under these two regulatory measures. And if you operate internationally, you must also consider GDPR and its effect on your data management processes.

Simple backup and recovery shifted to data protection as an all-inclusive term covering disaster recovery, business continuity, and of course backup. It's important to understand the differences and similarities of these functions and processes. At The CTE Group, we look at backup and recovery as a function, while disaster recovery and business continuity are processes that leverage the backup function. This means that backup must be handled appropriately for these processes to work as planned. One factor that exacerbates the challenge of data protection is the introduction of cloud. Cloud is a great resource for IT, and it can be a big differentiator for the business if employed correctly, but it requires you to ensure that the data on these cloud resources is fully protected according to your IT data protection guidelines.

IS HISTORY SET TO REPEAT ITSELF?

We tell all our clients, "Change for the sake of change will be disruptive and counterproductive." However, change with a strategy and plan tends to deliver the best outcomes. Looking back 10 years or more, backup was relatively easy. We pushed agents out to machines, backed them up, and made copies for disaster recovery. Today, we have data spread across multiple geographies, including data in the cloud. Maybe your organization wants to eliminate all on-premises data centers and is fully committed to cloud in a public/private mode. Or you may be in the hybrid cloud camp, with some of your data and compute split between your corporate premises and your cloud provider. Or, to add a bit more complexity, you may have opted for a multi-cloud approach, where you are using compute from one cloud and data in another in a heterogeneous architecture. If your existing backup infrastructure presents issues for your overall success, chances are that the additional layers of cloud will further extend this age-old problem. In that case, if you don't look at the bigger picture and your future needs, it's easy to fall back into old habits.

DATA SPRAWL: YOU CAN ONLY PROTECT WHAT IS KNOWN

Business units are just a credit card swipe away from creating their own infrastructure in the cloud without IT knowing about it. That presents significant challenges if that infrastructure touches critical primary data. IT can only protect what it's aware of, and shadow IT presents a serious problem for data protection. This is not a new challenge by any means, it's just more prevalent today. Back in the '90s, when I was a data center manager for an advertising firm in Chicago, I came across a network of computers in the client relations department that was operating 100% independently of IT. Their backup and recovery policies were ad hoc, the offsite transfer of data for DR was spotty at best, and to top it off this unknown network housed mission-critical client information. You're probably wondering how something like this can happen. The perception was that we in IT were not able to deliver at the speed of business, prompting the business unit leader to take matters into his own hands.

As you can see, this approach creates major gaps in IT's ability to protect these mission-critical assets. It wasn't long ago that we talked about "VM sprawl" as one of the top IT challenges. In the early 2000s, when virtualization started to hit mainstream acceptance, we found it very easy to create as many VMs as we wanted. That was, until we realized the effect of this practice on so many other IT functions, chiefly data protection. Similarly, data sprawl has become a serious issue today. Data can be located in multiple clouds, geographically dispersed across corporate data centers, on laptops and smartphones, and so on. It's staggering to think about the number of places your mission-critical data can exist today, and about your inability to know the location and mobility of that data. This lack of visibility presents serious issues in protecting the data and developing strategies to maintain continuity of operations for the business.

DISASTER RECOVERY

I have written and presented extensively on disaster recovery over the last 25 years. One of the most important decisions is defining *when* you declare disaster. That topic could be another white paper in itself, but I want to lay out some basic principles and definitions. You must fully understand the impact to the business if any of the systems become unavailable for a *predetermined* amount of time. One way to gather that information is to conduct a formal business impact analysis. Another is to simply identify the business units and their functions, and conduct meetings to understand the unique mission of each. In other words, what turns the business unit off? For example, if you are an airline, the mission of the business is to keep airplanes moving passengers and cargo safely and on time from one destination to another. What systems, applications, platforms, and so on support that mission? How long can the business tolerate inaccessibility to these systems, applications, and platforms before you must declare a disaster?

The time between when an outage occurs and the maximum time the business can tolerate that outage is called a *business Interruption.* Although that may seem rudimentary, it is an important factor in how you choose the solutions you use to protect your environment. You need to know that your storage and software solutions will make it possible to mitigate a disaster by recovering within the acceptable business interruption window.

As I mentioned earlier, at The CTE Group we believe that disaster recovery is a process that leverages the function of backup. DR typically leverages the outcome of the data protection function; that is to say, the successful backup of critical data. If the function is broken or does not achieve the desired outcomes, then the process of DR will break down during execution. The two are so closely tied to one another that it is important to create a solid foundational function with data protection to ensure that not only can it recover from a business interruption, but that your DR process allows you to recover after a declaration of disaster.

DON'T RETHINK STATEGY, THINK STRATEGY

Too many companies are using clever hooks to get you to rethink something. If your strategy was not working well before, rethinking it certainly won't make it any better—but developing a completely new strategy will. In thinking strategy, you need to ask questions like "What is our mission?" and "How do we want to show up to the business as a whole?"

Taking a new approach to your overall data protection strategy will help you overcome some of the hurdles that we discussed earlier. Let's look at some of the pitfalls of previous thinking or "rethinking." I will be the first to admit that back when I was running an IT team and backup and recovery, we looked at storage as a dumb resource. The intelligence was in the application we used to back up the data or the server that hosted the storage. And yes, we even treated the NACs (that's what we called the Network Appliance Corporation filers back in the '90s) the same way. That kind of thinking can only hinder your progress. There may be many who would argue with me, but I do believe that storage is at the heart of our environment today.

Storage is core to everything required by compute, network, memory, and so on. Without storage you have nothing but hope. Essentially, storage pumps all of the critical bits into and across the parts of the ecosystem (the body). Storage makes it possible to maintain multiple copies of data backup and protection elements used in the event of a failure or a full-on disaster. As with NetApp® solutions today, storage offers the means to overcome the hurdles of the past while taking advantage of modern resources, such as cloud.

Strategic Partnering

If you are a NetApp customer using 100% NetApp storage in your environment, then the data protection solutions from NetApp offer an amazing set of methods to help you meet and achieve your desired business goals and outcomes. If you're in a heterogenous environment, it's important to know that NetApp has very strong partnerships with the backup vendors you may be using or evaluating today, such as Commvault, Veeam, and Rubrik. You can expect the following benefits from these solutions, whether NetApp only or through a partner solution:

- Primary snapshot management
- Management of NetApp SnapVault® backup software and SnapMirror® replication technology
- Array-based cloning for dev/test and DR testing

Getting your arms completely around your data environment requires a strong data management platform. Whether it's NetApp only, or includes one or more of NetApp's data management partners, you benefit from using a single backup management tool for your entire environment. With NetApp, IT has the opportunity to significantly change the game and elevate its delivery to the business.

CONCLUSION

Going back to the title of this paper, *The Beat Goes On,* the reality is that we don't have to repeat history—we don't have to continue struggling with data protection. There are a number of things that we can do to alter our future course. I'm a firm believer in planning and strategy, and this is where I believe that IT can be one of the biggest partners to the business, by helping them understand the importance of compliance, data protection, and recovery.

If you haven't looked at your plan or strategy for backup and recovery, replication, disaster recovery, and business continuity in the past 6 months, now is the time to review it and ask yourself, your team, and your business unit leaders the hard questions, like "What grade would IT receive?" This kind of question isn't meant to set anyone up for failure, it's simply the best way to continue to deliver excellence

Here are a few closing thoughts you can take back to your IT team as you wade through the opportunities before you.
As you set out to review your existing plan and strategy for disaster protection and disaster recovery, or to create a new one, keep these points in mind:

- Conduct value assessments or business impact analyses in cooperation with the business unit leaders to better understand why the data is valued and where it is located.

- Start small and continue to grow and expand in order to have a full picture of what is required from a DP and DR perspective.

- Presenting the plan and communicating its value is just one step in the process of truly understanding the challenges you face in your organization. Make sure that the business is engaged throughout the process of creating the strategy. This makes buy-in more likely when the evaluation is complete.

- Do you have all the tools and resources to deliver on your stated strategy and plan?
  An important part of the equation is understanding your full capabilities, including staff, software solutions, cloud storage, and on-premises storage.

I have spent time with the team at NetApp over the last several months and have found their newly formed and existing partnerships to be quite impressive. As the strategic alliances between these companies continue to flourish and offer additional services to their combined customer bases, we believe that partnerships like these create impressive forward momentum for you, the customer. NetApp is looking at the bigger picture by establishing these relationships and helping its customers and prospective customers to achieve the goals and outcomes they desire from data protection management solutions.

Next Steps

Visit the NetApp website, or contact your reseller, integrator partner, or NetApp representative to learn more about the subjects covered in this paper. And be sure to check out the other papers in this series, *Beyond Modern Data Protection* and *Data Fabric Powered by NetApp: NetApp's Answer to the Data Protection Dilemma.*

The CTE Group

Practical | Direct | Candid

165 Caprice Court, Suite A
Castle Rock, CO 80109
info@thectegroup.net
720-924-8161