reducing risk of data loss and system downtime

NOVEMBER 2012

Bennett Klein & Jeff Drescher

CA ARCserve

Table of Contents

Executive Summary

In today's "always online" business environment, your company's success depends on its ability to protect and make available its systems, applications and associated data. IT departments, large and small, find themselves at the center of protecting these assets and making them available. Unfortunately, as important as this protection and availability might be to the business, IT budgets are not growing and businesses are certainly not creating less data or deploying fewer applications, operating systems or platforms – in fact the reality is the exact opposite. Adding to the complexity of this maze is finding the time in the 24x7 business day to properly ensure these systems are protected and the demands of the business are met with respect to recovery times and points in the event of a disaster.

With the increasing demands of the business, time and budget constraints along with the complexity of systems and infrastructure architecture, IT departments face a daunting task every day. The solutions chosen by IT to protect internal systems, applications and data should not add to the complexity and challenges of meeting the everyday demands of the business. IT requires solutions that are not only simple to deploy, use and fit into their budgets, but most importantly make systems, applications and data available anywhere, anytime and anyway possible.

Challenges Facing IT Today

Computing environments are dramatically different today than 10 years ago, and will look even more so 10 years from now. As the winds of technology have taken flight over the last decade, vendors continue to introduce solutions addressing specific problems within these changing environments, with little regard for the integration of these new technologies and the ability of IT to centrally gain control of the management of their environment.

Regardless of the size of the environment under management, be it a single location or a geographically dispersed one, IT requires solutions that meet the demands of the 24x7, always-online business - while fitting into the boundaries of tightening budgets. Whether these solutions are "on premise", "virtualized" "in the cloud" or any combination, is of little concern to most businesses; as long as the risk of data loss and system/application downtime is reduced so as not to negatively impact the top and bottom lines of the business along with employee productivity and even corporate reputation.

To help address these demands, technologies like cloud computing and server virtualization are being widely adopted due to their ability to dramatically reduce costs for the organization – the classic case of doing more with less. Unfortunately, these and many other cost efficient technologies inherently introduce additional complexities into the environment, especially when considering system, application and data protection capabilities.

Server Virtualization

Server virtualization has gained great traction within many organizations over the past few years for its ability to consolidate servers and reduce OPEX and CAPEX budgets, all while providing IT with the ability to further improve existing infrastructure investments. With multiple systems now consolidated and virtualized on a single server, applications running in virtual machines and data being created and stored on shared storage devices, the risk and exposure to system & application outages along with data loss are magnified significantly for the business.

As the winds of technology changed, the market saw vendors introduce solutions specifically to backup, recover and replicate these virtualized servers, virtual machines running on them and the applications/data stored within them. Many of these new solutions seem to have been created without regard for the existing IT infrastructure already in place. The net result of these "point products" is the reduction of the very savings that virtualization brought to the IT world when you consider one set of data protection solutions for physical environments and now a completely different set of data protection solutions, to perform many of the same tasks, but just for virtual environments.

Small Business Challenges

As technology and the delivery mechanisms of that technology continue to evolve, we are seeing that small businesses now have many of the same challenges as larger organizations.   Many of these small businesses now have similar "always online" requirements as larger organizations and the reduced costs of technologies over the years have resulted in some small business IT environments being even more complex than their larger enterprise counterparts.

Many small businesses have a variety of operating systems, applications and storage devices to protect and keep available, while at the same time being bombarded with so many technologies from many different vendors to manage them. Over time, these small business IT groups adopted disparate data protection solutions like backup, replication, image-based snapshots, high availability solutions, data deduplication and a host of others – while trying to somehow integrate them all on their own.

Challenges To IT In the End

Most IT organizations, regardless of size, continue to face reductions in staff and budget and are continually required to "do more with less". When selecting a data protection solution, IT is forced to balance comprehensiveness with simplicity to achieve their goals and many businesses even turn to outsourcing their data protection needs to managed service providers (MSPs).

At the end of the day, business is in business for the sake of business, not IT. While many challenges exist due to the demands that are put on IT for the protection of business systems, applications and data, it is up to IT to find solutions that provide the simplest and most powerful means of meeting these demands.

Section 2: Simplifying Data Protection

Prioritize Based On Business Value

Not all systems, applications and data are of equal value to your business. So why treat them the same? Simplifying your data protection strategy, regardless of how complex your environment, starts with prioritizing your systems, applications and data as they relate to their value to the business.

Only by first thinking about your business and the value of specific systems, applications and data on the business can you begin to properly define data protection requirements. Each business system or application should have a specific recovery time objective (RTO), the amount of time it takes to recover it, and a recovery point objective (RPO), the amount of data you are willing to risk losing. Take a hierarchical and logical approach to meeting different RTO and RPO goals – keeping things as simple as possible. For instance, your order entry system might be the lifeblood of your business while HR or legal systems and data might be a lower priority. Treat them and protect them accordingly.
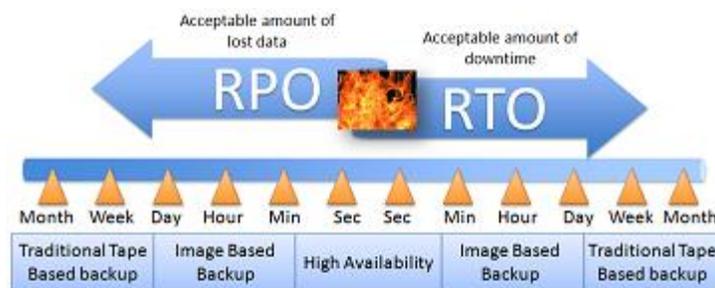
Ensuring Business Demands Are Met

After identifying and prioritizing your systems, applications and data, benchmark current performance to ensure the goals and demands of the business are being met. Identify gaps wherever they exist and understand what is missing and what is needed to meet these demands:

- Do you need faster or more frequent backups?
- Increased speed of recovery of certain or all systems?
- Understand how you recover a crashed server and how long it takes.
- How does data loss and system/application downtime affect your business?
    - How many sales and/or customers are lost?
    - What are employees doing when systems are down?
    - How much time does it take to re-enter lost data?

You get the idea. While this might seem like a tedious exercise, the data uncovered will save time and money in the long run for the business. Even if the time and resources cannot be spared internally to do this, there are many service providers and consultants that can perform this research to reduce the impact on staff resources.

What Can Be Done Immediately

Even before data is gathered, there are many things that can be done in almost any environment that will help reduce system, application and data loss risks while improving utilization of existing business resources.

1. Use Image-Based Backups. To help speed backup performance or to perform more frequent backups, consider utilizing an image-based backup solution to local disk – even as a complement to traditional file-based tape backups. Image backups to disk can significantly reduce recovery times compared to tape-based solutions.

2. Utilize Replication Along With Backup for Disaster Recovery. To comply with business demands, regulatory compliance and other regulations, most companies have traditionally made copies of their backups to tape just to be able to take them offsite for disaster recovery (DR) purposes. Even with all of the media attention on disasters, natural and otherwise, along with the importance the business puts on its systems, applications and data, many businesses still don't have a real DR plan or strategy and are at extreme risk. Consider the use of replication technology, in conjunction with your existing backup solution, to migrate backups offsite to the cloud for disaster recovery purposes - helping reduce the risk, cost and time associated with physical tape rotation. Cloud-integrated solutions offer a very affordable way to improve the protection of systems, applications and data.

3. Take it to The Next Level to Meet Business Demands. Most organizations don't have solutions in place to deliver high availability of business critical systems and applications. Performing basic backup does not protect the systems and applications from potential server and storage failures, which are far more typical than major disasters. Having to recover from a normal backup by re-installing everything from scratch can take many hours or even days, depending on the systems, applications and amount of data. Utilizing Bare Metal Recovery (BMR), cold standby, host-based high availability and server virtualization technologies can all help reduce downtime when business critical systems fail. With the advent of cloud computing, now

even small businesses can have enterprise-level data protection by using services from MSPs or public clouds for system failover and remote access in case of disasters or data center outage.

Whether you are a small business or a large enterprise and regardless of the steps you take, take steps now to prevent your business from suffering system, application and/or data loss.

Section 3: Considering a Solution For Your Business

The IT world is complex and there are literally thousands of applications and solutions from different of vendors that all promise to provide solutions to your problems. So, how do you cut through the marketing fluff and narrow that list down to a manageable size, especially when it comes to protecting your systems, applications and data? What type of a solution should you be looking for?

1. A solution offering multiple technologies to meet different RTO and RPO goals. It's simpler to deploy, manage and maintain integrated technologies from a single vendor than buying multiple point solutions that don't work well together or can be difficult to integrate.

2. One that supports a wide range of IT environments. Physical and virtual; servers and workstations; DAS, NAS and SAN; tape and disk; local and remote resources; etc.

3. A solution that fits into your environment. Find a solution that offers local, remote and cloud deployment and scales with the evolving needs of your business.

4. Find simple, yet powerful solutions. Ones that are easy to deploy, manage and maintain to help improve IT productivity. Look for centralized deployment, management and reporting.

5. Solutions that fit into your budget and business requirements. Solutions that offer flexibility in pricing and licensing to best match your environment and budget. Consider SaaS options too.

Summary

As computing environments evolve over time and the role of IT to support the demands of businesses continue to become more critical – finding and implementing data protection solutions that simplify the management of these critical assets does not need to be a complex task.   Most IT professionals agree that, regardless of the size of their organization, just having a basic backup product alone does not meet their needs. Seek simple, yet comprehensive solutions that meet the evolving demands of the business and eliminate hidden costs. Look to reduce complexity by minimizing the number of point solutions by working with a data protection partner that delivers on as much of your business' needs as possible.