WHITE PAPER

Best Practices in Business Continuity and Disaster Recovery

Sponsored by: Riverbed Technology

Laura DuBois

February 2011

EXECUTIVE SUMMARY

Business continuity and disaster recovery can mean either life or death for a company. In the event of a disaster, inadequate planning and/or technology deployment can compromise a return to operations and bring financial downfall. With this in mind, we note that operational continuity and recovery objectives continue to increase in priority for commercial and government entities alike. Recovery objectives once measured in days or hours are now measured in seconds or minutes. This is motivated by increased business reliance on technology and a diminishing tolerance for downtime and its financial impact. This downtime can also bring unwanted visibility by customers, partners, stakeholders, competitors, and the industry at large — and threaten the credibility of a firm.

IDC research highlights a number of practical challenges frequently at odds with a firm's continuity and recovery objectives. Most commonly, issues such as data volume and annual growth, network bandwidth and latency, and infrastructure costs inhibit a firm's move to a best practice scenario for meeting business service-level agreements (SLAs) on availability and recovery. Other technology trends such as server virtualization and infrastructure consolidation further exacerbate continuity and recovery objectives as more data is increasingly resident in fewer physical assets or locations.

In 2010 alone, there were over 80 disaster declarations in the United States, according to the Federal Emergency Management Agency (FEMA). An even larger number of security, technology, network, and telecommunications outages and disruptions also occur annually. All businesses experience these conditions. In preparation for a major outage, disaster, or disruption to a corporate IT network, businesses find that one of the most profound hurdles to data protection and recovery is moving terabytes of data across a congested and shared corporate WAN. WAN optimization solutions introduce both network visibility and accelerated data replication that fit into existing storage and backup processes. These solutions can support replication of data at high speeds and transfer huge data loads over the WAN to accelerate recovery point objectives (RPOs) and recovery time objectives (RTOs) and meet even the most stringent demands of the business.

This paper highlights the challenges to and best practices for continuity and recovery. It then highlights the strategies that Riverbed Technology, a WAN optimization solution provider, enables firms to employ to meet their recovery requirements. Riverbed's breadth of solutions can optimize continuity and recovery across a range

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

of backup, replication, and cloud storage mechanisms without disrupting a firm's current infrastructure — ensuring the protection of existing investments. As a result, Riverbed offers a firm both choice and control as it evaluates and takes different approaches to meeting business SLAs for given applications, datacenters, or distributed environments.

SITUATION OVERVIEW

Business continuity and disaster recovery are words often used interchangeably, but they are different in terms of both policy and technology.

Business Continuity

At its most simplistic level, business continuity is the ability to maintain operations/services in the face of a disruptive event. Business continuity requires the availability of computing, application services, physical network access and network services, as well as user/client access to this infrastructure. Maintaining continuity in operations and services, including systems such as Web servers, email, critical databases, and so forth, requires specific technology. This technology and infrastructure can include virtualization, clustering/failover/failback, server hardware, network and networking services, remote datacenter facilities, replication services, and redundant shared storage. Depending on the type of event, continuity of a given application is achieved by failing over its services and user/client access locally within the same datacenter or to a remote, physically disparate datacenter. With business continuity, the failover of a service is measured in seconds or less. Backup technologies, including those that rely on disk as a backup target, cannot provide this level of continuity of services. Backups, in order to be used, require a restoration process and are typically used for disaster recovery purposes.

Disaster Recovery

Disaster recovery is a broad concept that can include recovery of people, facilities, and the like. For the purposes of this paper, disaster recovery is the coordinated activity of recovering IT systems following the complete or partial loss of a site due to a natural disaster or a security event. Depending on the extent of the disaster, disaster recovery can be achieved by restoring systems at an alternative site or within the same site using alternate equipment. Disaster recovery requires extensive manual methods to bring the IT environment up to an operational state. For example, services need to be reestablished, servers rebuilt, applications reinstalled, and data restoration completed. Infrastructure used for disaster recovery can include virtualization, server hardware, network and networking services, remote datacenter facilities, replication, backup to disk, backup to tape, and tape vaulting. While business continuity is measured in seconds, disaster recovery is typically measured in hours or days. However, some well-designed disaster recovery plans incorporate highly automated failover to designated disaster recovery hot sites. In these cases, through the use of the right technology, recovery can be achieved far more quickly.

Changing Landscape for Business Continuity and Disaster Recovery

The increasing numbers of physical disasters and security concerns have forced firms to place a higher priority on continuity and recovery. There is no longer any tolerance for downtime because of the financial implications with tier 1 applications. There has been higher visibility at the C level and with key stakeholders because no executive wants to influence stock price declines or loss of key stakeholder confidence. If the CEO cannot tolerate his email being down, consider his reaction when other critical applications are disrupted, impacting the bottom line, sales orders, and so forth. Also not to be overlooked is the impact of regulatory compliance. Consider the following statements:

- **C-level visibility.** "Replication and [disaster recovery] are very high priority right now. We had a data corruption issue in our production Oracle financials database … the whole scenario put the fear of God in the executives." *(Manufacturing)*
- **Risk mitigation.** "Within 24 hours we have to be back up and running. We have regulatory issues with cancellation notices and various things that need to be done within a certain period of time, and if we couldn't produce certain documents within that period of time, then that extends our exposure." *(Insurance)*
- **Regulatory compliance/cost of downtime.** "The screen-based trading really can't be down. We are required by the SEC if we are down for 30 minutes to shut our doors, so there really is no acceptable downtime." *(Financial Services)*
- **Cost of downtime.** "If we are looking at 24 hours to recover an environment, we are stranding tons of food on conveyors that we can't restock. We are throwing away anywhere from $300,000 to $500,000 of food on a given day if we lose our ERP system. Even an hour outage can be a disaster. We need to be under 10 minutes." *(Consumer Services)*
- **Changing objectives/cost of downtime.** "We needed to upgrade the open systems to go from 30 minutes down to 15 seconds. Fifteen seconds in my organization can mean, literally, billions of dollars. We clear $5 trillion a day." *(Financial Services)*
- **Unexpected events.** "We had a failure event that took down both the emergency power and the site power from the street. The hotel had to be closed for five days. That was devastating. It had never happened in this town before, and it happened to us." *(Hospitality)*

Challenges with Successful Business Continuity and Disaster Recovery

Business continuity and disaster recovery are time-consuming, resource-intensive processes. Firms face many challenges with putting the proper planning, people, and technology behind these programs. The effective implementation and operation of business continuity and disaster recovery is stymied by the following:

- **Capital costs.** This includes hardware, network infrastructure, remote disaster recovery sites, and infrastructure at remote offices.

- **Differing SLAs.** Not all data and systems are equal. Tier 1 and tier 5 applications have different SLAs and require different technology to meet the objectives.
- **Data growth.** On average, storage volume grows 52% annually. This increasing volume of data is at odds with congested WANs and/or LANs.
- **Network latency and bandwidth constraints.** While network costs tend to come down slightly over time, price declines are not in alignment with data growth rates.
- **Infrastructure disruptions.** This includes components outside of a firm's immediate control, such as power, cooling, and telecom services.
- **Project management component.** Business impact analysis is time consuming and means translating business needs into IT implementations and getting accurate cost of downtime implications estimates.
- **Adequate planning and testing.** Effective continuity and recovery require planning for an actual event. The preceding factors often stymie frequent testing.
- **Increased IT complexity.** New technology trends such as virtualization and cloud computing can increase complexity from orphans, VM sprawl, and image- and system-level recovery.
- **N-tier application architectures.** Certain applications (i.e., SharePoint) require consistent recovery of several tiers.
- **Breadth in recovery.** Continuity and recovery involve many IT groups and components, including networking, compute, services, applications, and data.

CURRENT BEST PRACTICES IN BUSINESS CONTINUITY AND DISASTER RECOVERY

Over the past several years, firms have employed a set of emerging best practices to effective business continuity and disaster recovery. Firms are taking on the following best practices with their business continuity and disaster recovery programs:

1. Assign continuity and recovery professionals to develop plans and coordinate between business and IT.
2. Prioritize and tier applications and establish SLAs for each tier in concert with the line of business (LOB). Identify cost of downtime for each tier or application.
3. Develop service catalogs that define set SLAs from which the LOB can choose.
4. Ensure infrastructure redundancy (networking, power, cooling, telecom).
5. Run periodic testing of plans, ideally quarterly, with published results and vulnerability patching analysis.
6. Conduct an annual review of business continuity/disaster recovery goals/plans with the LOB, including evaluation of technology to achieve SLAs for different application tiers.
7. Deploy tools to identify vulnerabilities and virtual server orphans (i.e., systems with no SLA or protection schema).

8. Evaluate and deploy optimization technologies such as deduplication to address data growth, network latency, and congestion issues.
9. Consider the role of cloud — public, private, or hybrid in continuity and recovery.
10. Evaluate disaster recovery infrastructure and network resources and plan for future requirements.

RIVERBED'S STRATEGY FOR BUSINESS CONTINUITY AND DISASTER RECOVERY

Riverbed is a provider of IT performance solutions for networks, applications, and storage. It provides comprehensive WAN optimization and cloud storage solutions for a number of problems that prevent enterprises from storing data in the cloud and sharing applications and data across WANs anywhere in the world. Riverbed's WAN optimization and cloud storage solutions help customers overcome constraints in achieving their continuity and recovery objectives.

Riverbed's unique approach does not require firms to rearchitect their infrastructure around the Riverbed technology. Instead, Riverbed fits within the existing environment, giving firms the flexibility and choice to use Riverbed solutions in a number of different ways. Organizations can use Riverbed across different environments from local backup in the branch to private cloud consolidation to migration to a public cloud service — or any combination. This gives firms the freedom to pursue what is right for their business and make changes as demands dictate.

Riverbed solutions allow companies to scalably leverage their WAN for high-performance backup and/or replication or simply and efficiently utilize cloud storage as a backup or archive target. Firms can seamlessly integrate Riverbed solutions into their existing infrastructure to maximize their continuity and recovery capabilities and reduce costs, delivering huge improvements to their availability, recovery, and storage operations.

Riverbed's Steelhead WAN optimization products reduce bandwidth requirements for backup and replication across the WAN, increase throughput on high-latency links even in the face of packet loss, and, with quality of service (QoS), provide control over prioritization of disaster recovery versus other business network traffic. They also offer significant performance improvements above and beyond storage-level deduplication and compression.

Riverbed's WAN optimization solutions aid in recovery and business continuity by:

- **Reducing** the amount of data transported over the network for either backup or replication processes. Thus, Riverbed shifts the network from a barrier to an enabler in moving data securely offsite.
- **Prioritizing** WAN traffic, thus increasing replication and backup throughput and reducing bandwidth requirements. This empowers a firm to protect more data, more often and recover faster.

- **Discovering** systems to be protected and critical interdependencies, thus mitigating vulnerabilities in protecting and recovering data.
- **Monitoring** data protection processes to ensure they complete, **identifying** outages to mitigate vulnerabilities and risk, and **diagnosing** root problems for quicker recovery.

Riverbed's cloud storage solutions enable firms to utilize public and private cloud infrastructure with no negative impact to the business. With a Riverbed approach, organizations can virtualize applications and improve performance levels so that employees can be as productive as if everything were local. The consolidated cloud infrastructure is enhanced by Riverbed WAN optimization to introduce cost savings and performance benefits so that businesses can operate more efficiently. The Riverbed cloud storage solutions accelerate movement of files, data, servers, and machines to public and private clouds while freeing up network bandwidth. Data transfer, access, and migration times are dramatically shortened.

Riverbed's cloud storage solutions aid in recovery and business continuity by:

- **Accelerating** data access and movement of virtualized machines to private and public cloud infrastructure
- **Reducing** the bandwidth needed to support branch offices and datacenters for volume- and redundancy-intensive backup data
- **Removing** WAN performance barriers, enabling the effective use of cloud services
- **Integrating** WAN optimization technology with existing hardware appliances, software, and virtualized platforms
- **Migrating** backup and archive processes to a cloud storage environment for capital and operating cost reductions

Protecting the Datacenter

Many firms, in particular large enterprises, deploy remote replication to replicate data between datacenters. Replicating data between datacenters may involve unidirectional or bidirectional replication or make use of a three-way replication process. Alternatively, WAN-based backup from one datacenter to another or from datacenter to cloud may be deployed. In any of these scenarios, limited bandwidth can really constrain the ability to back up or replicate a lot of data on the WAN over the network. For replication between large datacenters, there may be adequate rated bandwidth capacity to keep up with the changing data, but due to high latency and/or packet loss and retransmission, firms may not be able to effectively use the capacity. There is a certain amount of management overhead and error correction in most storage protocols, and the further you need to go, the worse this slows things down. Also to be considered is adequate distance between sites to ensure no regional disaster affects both the primary site and the recovery site. Some firms are starting to also consider the use of cloud services to copy data from a major datacenter to a third-party public cloud for the purposes of protection and recovery.

Riverbed solution: Riverbed Steelhead appliances make use of existing WAN-based backup or replication processes and network infrastructure, but they empower firms to protect more data, more often (for a better RPO) and recover faster (for a better RTO) across the WAN. Riverbed's Data Streamlining on bandwidth-constrained connections can remove up to 60–95% of the traffic by essentially deduplicating data on the WAN, recognizing data that has been sent before and offering it up locally from the Steelhead appliance in the immediate datacenter. Only new data goes across the network, and this is also compressed for additional savings. The Data Streamlining feature can self-tune each connection dynamically depending on how much pressure it's receiving to increase throughput versus reduce bandwidth requirements. Riverbed's Transport Streamlining and Application Streamlining features deliver maximum performance by optimizing the operation of core storage protocols as they attempt to move data across the WAN. These features can enable data transfer to ramp up much faster and fully utilize allocated capacity, even in the face of congestion and loss. This is especially important in quickly draining data from the storage array or software replication cache to avoid failing asynchronous replication jobs. Riverbed not only has created a solution that drops into place without changes to storage arrays or backup/replication software but also has certified its products with the major storage vendors. Riverbed has implemented these solutions with EMC, NetApp, IBM, Dell, HP, and more.

Protecting the Branch Office

Firms are taking several approaches when it comes to protecting data in remote and branch office locations. Some consider consolidating infrastructure back to the datacenter, thus minimizing the amount of data stored locally. Others rely on local backups. A third group of firms are considering the use of either public or private cloud services to protect data in edge locations.

As datacenters continue to consolidate, the number of remote and branch locations continues to expand. Depending on the size of the firm, the number of remote and branch locations can go from hundreds to thousands. Some firms will employ local data protection processes for each location and may move tapes offsite. However, according to IDC research on branch office strategies, a majority of firms are centralizing backup and replication processes to a core datacenter. IDC research highlights a myriad of different and limited networked connection types for edge locations to core datacenters. In these edge-to-core use cases, limited WAN bandwidth can profoundly constrain the ability to backup or replicate a lot of data on the WAN. Data transfers slowly trickle over small pipes from branch offices to the datacenter. The cost of network connection upgrades typically means selectively choosing networks to upgrade. And with average data growth rates, these same networks may require upgrading again in a few years' time.

Riverbed solution: Steelhead appliances eliminate a firm's reliance on physical shuffling of tapes to move data offsite. For firms using WAN-based backup or replication, more data can be protected, more often and with faster recovery over the WAN. Again, firms benefit from Adaptive Data Streamlining on bandwidth-constrained connections. Steelhead appliances are essentially deduplicating packets over the WAN, recognizing data that has been sent before and offering it up locally from the Steelhead that is local. Only new data goes across the network, and this is also

compressed for additional savings. Given different connection types, their adaptive features can self-tune each connection, dynamically balancing throughput versus bandwidth requirements. A common challenge in remote locations is the lack of technical personnel. For firms with limited IT personnel in remote office/branch office (ROBO) locations and a desire to limit physical hardware in distributed environments, a Virtual Steelhead solution can be deployed. Virtual Steelhead runs inside a virtual machine and can be managed by standard virtualization tools to enable centralized control. Organizations considering consolidation of their data to a private or public cloud can leverage Riverbed's cloud solutions.

Leveraging the Cloud

Another disaster recovery scenario that firms are deploying is the use of public cloud services for either backup or archiving. According to IDC research, firms are moving to public cloud storage services to reduce capital expenses, stand up services more quickly, and maximize IT talent for more strategic tasks. However, one significant hurdle to the adoption of these services is the data volume versus data pipe problem, in particular for bulk data movement such as an initial backup or a full restore process. Data seeding services and appliances as well as client-side data reduction techniques have been used in part to mitigate these challenges. But client-side deduplication does not address the challenge of the initial bulk backup required. In addition, public cloud storage services have been slow to deploy target-side deduplication.

Riverbed solution: For environments that want to send their backup data to public cloud storage, Riverbed's Whitewater solution can be used to send backup and/or archive data to a third-party cloud in an efficient, cost-effective manner. Riverbed Whitewater appliances augment existing on-premise backup methods and integrate with existing backup software. Firms can send data offsite to the public cloud of their choice without any changes to their current processes. The backup or archive data will be deduplicated in the network using Riverbed's deduplication algorithms. A third-party cloud such as Amazon S3 serves as a quick-to-deploy target for a firm's existing backup and archive tools. In moving data to a public cloud, firms need to consider solutions that can reduce network bandwidth and security issues by employing deduplication and encryption respectively. Using these technologies can improve performance and reduce the space required up to 30x, simplifying connectivity to elastic cloud storage services while mitigating data loss risks.

The Riverbed Cloud Steelhead solution is a cloud-intelligent WAN optimization solution to be offered for Amazon Web Services and other providers to come. Cloud Steelhead transforms an Amazon cloud into an extension of the datacenter by eliminating the barriers to enterprise-class public cloud deployments. Cloud Steelhead combines the speed and simplicity of a Steelhead appliance, subscription pricing, and a host of intelligent features like transparent interception. Organizations can easily install and scale Cloud Steelhead within Amazon Web Services' Elastic Cloud Compute (EC2) and Virtual Private Cloud (VPC) environments.

CONCLUSION

Firms that do not employ business continuity and disaster recovery do so at their own peril. CIOs and IT managers who do not plan for a range of disruptions to business operations can compromise a return to operations and bring financial downfall for their firm. This paper highlights some best practices for continuity and recovery. Firms that are serious about achieving business continuity and/or disaster recovery must consider IT performance solutions such as those provided by Riverbed. The use of performance accelerators will optimize continuity and recovery across a range of backup, replication, and cloud storage mechanisms without disrupting current infrastructure — ensuring the protection of existing investments. Riverbed's offerings provide both choice and control as firms take different approaches to meeting SLAs — to ensure that business operations remain viable despite unanticipated outages or disruptions.