After September 11: Lessons on Planning and Implementing Business Continuity

A White Paper

By Charles King

The Sageza Group, Inc.
March 2002

The Sageza Group, Inc.
836 W El Camino Real
Mountain View, CA 94040-2512
650·390·0700 fax 650·649·2302
London +44 (0) 20·7900·2819
Munich +49 (0) 89·4201·7144

sageza.com
info@sageza.com

After September 11: Lessons on Planning and Implementing Business Continuity

ABSTRACT

With the perspective on the events of a mere six months ago, this paper examines what enterprises and their vendors are doing differently to ensure data continuity since September 11, 2001. As the essential foundation for business continuance, data continuity provides ongoing access to business-critical information. The Sageza Group worked with EMC, its customers, New York professionals, customer service, and headquarters staff to explore what they learned and what it means to organizations planning for enhanced business continuity.

What follows is a high-level discussion of some of the human, organizational, and ethical elements that need to be considered in implementing effective business continuity plans. It does not purport to be a comprehensive disaster recovery (DR) planning guide, but it does consider issues critical to DR processes.

Data replication, both local and remote, is a central element to business continuity planning. The focus should be on rapid restart. One key is to integrate these capabilities, and the ability to manage them, into the DR plan. Another key is to evaluate these capabilities in making storage decisions. This evaluation should include the technology, the ability to manage and automate it locally and remotely, and the vendor's ability to service and support it and the company in the event of a disaster. Despite tight IT budgets, we believe that postponing the implementation of a rapid restart data continuity plan is not a wise option for enterprises to pursue.

After September 11: Lessons on Planning and Implementing Business Continuity

TABLE OF CONTENTS

Lessons Learned

Sageza identified eight key lessons concerning business practices that we believe are essential for completing disaster recovery plans and maintaining business continuity. The events discussed largely derive from discussions with EMC's customers and staff, both in New York and in Massachusetts. We believe these company experiences provide valuable insight to enterprises as they plan for business continuity in 2002 and beyond.

The Eight Key Lessons Learned

1. Automate for Rapid Restart

One EMC senior executive arrived in New York within twenty-four hours of the attack to help coordinate operations, but found himself spending the next two days simply listening to employees talk about their experiences. He quickly realized that it was far more important for him to listen and let employees know how much they mattered to EMC than it was to follow his original assignment. The employees *needed* to talk about what happened to them, and to their families, friends, colleagues, and customers.

Dedicated and talented customers and vendors worked under extreme conditions. They had little or no time to sleep, and in some cases no reasonable way to get home and back. After working thirty-six or more hours, under the weight of everything that happened, the judgment and abilities of even the best people suffered. Global vendors such as EMC had the advantage of using expert staff stationed worldwide to assist, but most customers did not have that luxury. Their people were there doing everything they could to ensure business continuity. But in many cases, there was simply no way for them to get to the recovery site or get the information or equipment to that site.

The lesson is to automate the replication and recovery processes. When employees are stressed and optimal decision makers are not available, the chances of human error and elongation of the recovery process grow exponentially. Clients should demand that their vendors provide solutions that automate these critical processes.

2. The Formula for Business Continuity

(Duplicate + Disperse) (Data + People) = Business Continuance

In the days and weeks following disasters, whether earthquakes in California, hurricanes in Florida, floods in London, or the events of September 11, an essential constant emerges. Enterprises that had implemented plans to duplicate and disperse their data and recovery staff prior to the disaster maintained better qualities of business continuity, and recovered more quickly, effectively, and completely than those that did not. We believe the "formula" depicted above is an effective indicator for considering enterprises' chances for successful rapid recovery from wholly unanticipated disasters. In many ways, duplicating and dispersing data is easy. There are well-tested solutions for managing remote replication and rapid restart at second and even third sites. Companies must also consider dispersing their staff, a potentially expensive proposition but one that enterprises cannot afford to ignore.

3. Plan for Flexibility

"Find your people" is the mantra for everyone immediately after any major disaster. Amidst the awful chaos within and around the World Trade Center, businesses first accounted for their employees and then began evacuating their offices. Companies also instituted disaster recovery plans, began deploying or diverting staff to remote recovery sites, and started data

restoration or failover processes. However, efforts of every kind were made more complicated by ongoing problems in New York's telecommunications system. Cellular traffic was hugely impacted by the collapse of the World Trade Center towers, where a large number of cellular antennae were located, and landlines were frequently overwhelmed by traffic and power outages.

By a serendipitous chance, employees at EMC's Philadelphia office discovered that their calls were getting through to New York while calls within New York were not. This alternative helped tremendously in those first few hours, enabling EMC employees to contact their families, and to do the same for the company's customers and partners. Some vendors and customers discovered and used similar techniques, in some instances routing calls through offices in London and California to assist in these tasks, while others utilized highly effective satellite phones and Blackberry devices. Flexibility, imagination, and a willingness to search out unconventional solutions when plans go awry were the keys to these successes. So, plan and test alternative telecommunications routes, but even as you do that, consider what to do in case those routes are also disrupted.

4. Empower Staff to Speed Recovery

It sounds simple but employees are every enterprise's greatest resource, and giving staff on the ground real authority benefits both vendors and customers. EMC empowered its headquarters staff and customer service staff to place people and equipment where they were most needed. Importantly, while the staff at headquarters communicated extensively with staff and customers in New York, they had the luxury of distance that enabled a degree of perspective. They ordered equipment directly from the factory and had it

Case Study: Commerzbank

With over $21 billion in annual revenues, Commerzbank AG is the world's sixteenth largest lending institution. The company's five U.S. branches handle about $30 billion in transactions per day. Its North American headquarters, on the 33rd floor of Two World Financial Center, stood roughly 300 feet from the World Trade Center. At 8:48 a.m. EST, when American Airlines Flight 11 crashed into the Trade Center's north tower, most of Commerzbank's 400+ headquarters employees were either on premises or en route to work. After United Airlines Flight 175 impacted the south tower at 9:03 a.m., the company successfully accounted for and evacuated all of its personnel. Fortunately, a group of key management and IT staff were able to get to Commerzbank's disaster recovery site in Rye, New York, 32 miles north of Manhattan.

Like virtually every lending institution, Commerzbank is extremely data conscious. The company has had a formal disaster recovery plan in place since 1997. Early in 2001, Commerzbank decided to move from tape to disk remote mirroring for disaster recovery for its critical applications. On September 7, 2001 Commerzbank completed the first phase. The EMC SRDF implementation of the critical data went live on that day. Two terabytes of Windows NT-based and VMS legacy data were not part of this phase and continued to use tape for DR purposes.

When Commerzbank's disaster recovery team arrived in Rye, the bank found that SRDF worked as expected and that the data in Rye was up to the transaction and ready for access. The team worked to ensure that its infrastructure was ready to provide effective operations. Within four hours, the bank's new data center became its primary data center running these applications as effectively as the one near the World Trade Center. The company has stated publicly that if its tape-only system had been in place on September 11, their initial data recovery phase would have required at least twenty hours to complete. Commerzbank's IT team was aided by EMC customer service representatives who worked alongside them for more than a week. About 90% of the company's stored data was available within seven to ten days.

delivered within twenty-four hours. They located and secured equipment en route to other customers (in some cases even off their loading docks) and rerouted it to critically impacted clients. In one case EMC secured a used VAX server so a customer could get its application back online.

In other cases, EMC (and we believe other vendors had comparable achievements) delivered fully configured and tested SANs, some quite large, to customers' new recovery sites. On the client side, customers empowered their own staffs to make quick decisions with vendors to establish priorities, confirm configurations, allocate personnel and get the job done quickly and professionally. In the overwhelming majority of cases, experienced staff will make good decisions. The key is to allow them to step outside traditional bureaucracy when those processes impede rather than enable effective solutions.

5. Tape is Untimely and Sometimes Inaccessible

Databases become corrupted, software has bugs, staff members make errors, and hardware breaks. Those are some of the reasons companies backup their data. But this discussion has evolved to be less about backup and more about recovery or restart. Tape recovery is often slow and resource-intensive. As a result of that and the wide availability of point in time disk replication, companies more and more are using disk for rapid recovery. Sageza is aware of new software that manages and schedules data replicas, automating and simplifying these tasks.

In the event of a disaster, tape can take days to restore compared to minutes or hours for remote disks. In New York, some companies were still restoring from tape months after September 11. In some cases, companies stored their backup tapes in basements or other parts of buildings that were destroyed. In other cases, staff simply could not get the tapes to the recovery site, or get people to the recovery site with tapes in hand. Tape continues to be important for some specific processes, but overall, we believe that disk-based replication technologies, both local and remote, are far more capable of quickly restoring business processes in an automated, synchronized, and timely manner than are tape-based backup solutions. For this reason, Sageza believes that enterprises would be wise to explore disk-based replication solutions for local as well as remote rapid restart scenarios.

6. Harden Supply Chain Relationships for Survival

Many forward-looking companies establish close electronic relationships with their supply chain partners to save time and costs. Customers that were able to failover to alternate sites quickly learned how dependent their internal processes were on external processes. Disasters clarify a simple truth: that in today's highly connected, global business environment, supply chains extend well beyond their traditional enterprise borders. Any interruption in the flow of information in a business process, whether internally self-contained or extended throughout the supply chain, has ripple effects across the companies involved.

Many enterprises are working with their supply chain partners to design and deploy robust, hardened business continuity plans that reduce the risk of significant down time by establishing specific, demonstrable performance guidelines for all involved parties. Organizations recognize the dependencies between transaction-based and decision support systems, and must extend their business continuity plans to include external dependencies. Duplicating and dispersing information must be done in a synchronous and synchronized fashion to enable rapid business resumption at alternate locations. Considering the potential benefits such integrated solutions offer, we believe these plans will become increasingly common features of the supply and implementation landscape.

7. Degrees of Separation

In the last three to four years, fundamental changes have occurred in the ways enterprises are practically and strategically deploying their data centers. Growing numbers of companies have consolidated data centers, and in many cases implemented or planned to implement individual, hardened data centers. While we believe this consolidation is likely to continue, other enterprises have begun investigating a shift from a passive to an active data center model. In an active model, two or more centers individually support production while acting as recovery sites for the other centers involved. While most large companies expect to have their own second data centers to guarantee access to business-critical data, many others will contract with DR service providers as second sites.

Active data centers duplicate and disperse both critical data and staff, enabling crucial business processes to continue despite natural and other disasters. Additionally, active data centers can help enterprises ensure that they have few if any idle assets. In fact, along with data backup and disaster recovery, some companies are also utilizing active secondary sites for application development and testing. The active model's ability to help ensure business continuance while providing new leverage points for enterprises' infrastructure investments will help drive its broad acceptance.

But even these customers are looking beyond a second data center. Some are planning a third center on a different continent so that they can continue to operate effectively even if all air travel to one company site is halted for days. Most organizations may not need to plan for the third data center across the ocean, but they do need to plan for the possibility of substantial travel disruption.

Many businesses' recovery facilities were located nearby in New Jersey, and if the wind had blown the cloud of debris toward New Jersey instead of out to sea, those facilities might have been endangered by choking dust that could have compromised ventilating, heating, and cooling systems and driven people from their buildings. At one site located near Ground Zero, an EMC Professional Services employee was confined in a data center where the building's air conditioning units had failed due to dust and debris. He spent the next thirty-six hours moving portable air conditioning units from room to room to help cool the equipment, and emptying the constantly filling water trays. This is an admittedly remarkable if not singular example, but it illustrates the fact that a data facility, like a supply chain, is subject to a wide variety of influences, some apparent and others obscure.

To our way of thinking, success will be found by developing data infrastructure solutions that are robust, automated and flexible.

8. Select the Right Disk Remote Copy Solution

Companies today are ensuring data consistency among interdependent databases and studying the implications of synchronous versus asynchronous remote copy. There are fundamentally two choices for remote disk mirroring: synchronous and asynchronous. Synchronous remote copy guarantees that transactions at the remote site are fully up to date, but in distances over 400 miles the process will introduce transaction latency because of the speed of light. Asynchronous remote copy mitigates the latency, but leaves the secondary site anywhere from two to fifteen minutes worth of transactions behind. In the event the primary site goes down, the company will lose that data and may not be able to recover it. If data loss is unacceptable, companies need to implement synchronous remote copy.

Some enterprises combine both technologies, with a relatively short distance to a synchronous site and a longer distance to an asynchronous site, allowing data to be quickly brought up to date at the far site. This provides the business with no data loss over long

distances, and business resumption within minutes. It is also important to understand database interdependencies in remote copy transactions. For example, if a sales transaction updates the customer database and the accounts receivable database, these databases are intrinsically linked and must be kept consistent. If a company loses one portion of the transaction, all of the databases become inconsistent, a database recovery must be performed, and some data may be lost. Many business applications span multiple storage systems and run on top of databases. Databases have transactions that must occur in a specific sequence. In the event of a failure at the primary site, the remote copy software must be smart enough to ensure that dependent write consistencies be enforced at the remote location. In this way, it ensures data consistency and application integrity.

Summary

"Duplicate and disperse to enable rapid restart" may be the essential business technology lesson of September 11. The duplication of business-critical data and processes in widely dispersed facilities with dedicated teams of personnel provides what we believe is a robust framework for disaster recovery and business continuity. These capabilities need sophisticated automation and remotely accessible centralized management across the entire enterprise. As such, we see this model as one that companies will have to adopt or at least seriously consider as they move ahead. After all, the most business-critical issue for virtually every enterprise is its ability to continue operations regardless of circumstances. In the end, it is the enterprise itself that is enterprise-critical, and its information is its lifeblood. The enterprise should remain the key focus of every disaster recovery implementation. Build in flexibility and alternatives. Consider the humanity of your staff as well as their business and technical expertise. Without that focus of effort, enterprises will find it difficult to survive events far less catastrophic than the terrorist attacks in Manhattan and Washington, D.C.