APPLICATION NOTE

Disaster recovery and business continuation: planning for success

Considerations for cost-effective data center protection and business continuation

APRIL 2004

1 INTRODUCTION

What constitutes a disaster? And more important, how well can you survive one if it strikes your business?

No one would argue that hurricanes, earthquakes, fires, floods and terrorist attacks are all disastrous events. Such events are highly publicized because of their great impact on human life and potential to destroy industry and commerce.

Businesses that encounter disastrous events are put to the test to see if they can survive. According to North American Emergency Management, 60 percent of such businesses do not re-open their doors. (http://www.naem.com/planning/html/planning.html) Those that do recover frequently face significant expenses and cannot recoup business opportunities lost during the recovery period. In addition, their customers may defect to competitors; a corporation could suffer diminished brand equity and overall reputation. In some cases, these combined effects could even lead to the demise of the organization.

While these highly publicized events make headlines, they actually are in the minority of outages that plague modern business. Most outage threats come on a smaller scale. System downtime is more likely caused by hardware failure, application failure and human error. These types of failures may cause your information to become unavailable and leave your customers out of touch.

How a company survives these events may very well depend on how well it has prepared itself. Much of the potential failure stemming from an outage, whether disastrous or not, can be averted with proper planning, implementation and testing. With thoughtful business continuity planning that includes people, facilities, data, systems and processes, an organization can mitigate the possible risks of a service interruption.

This paper will look at these critical processes and how they affect your IT systems as well as your overall business performance. Regardless of the size of the business, by taking the necessary steps to support business continuance today, you can position your company for unexpected disruptive events — both large and small — for today and tomorrow.

2 DISRUPTIONS COME IN ALL SIZES

Headline disasters get everyone's attention. The truth is, however, that disruptive events can range from a small hardware failure to events that can only be called catastrophic.

In fact, the headline-making disaster is the exception. A breakdown of the causes for application downtime actually looks like this:

> Forty percent operation error
> Forty percent hardware error
> Twelve percent application failure
> Five percent disaster
> Three percent other environmental

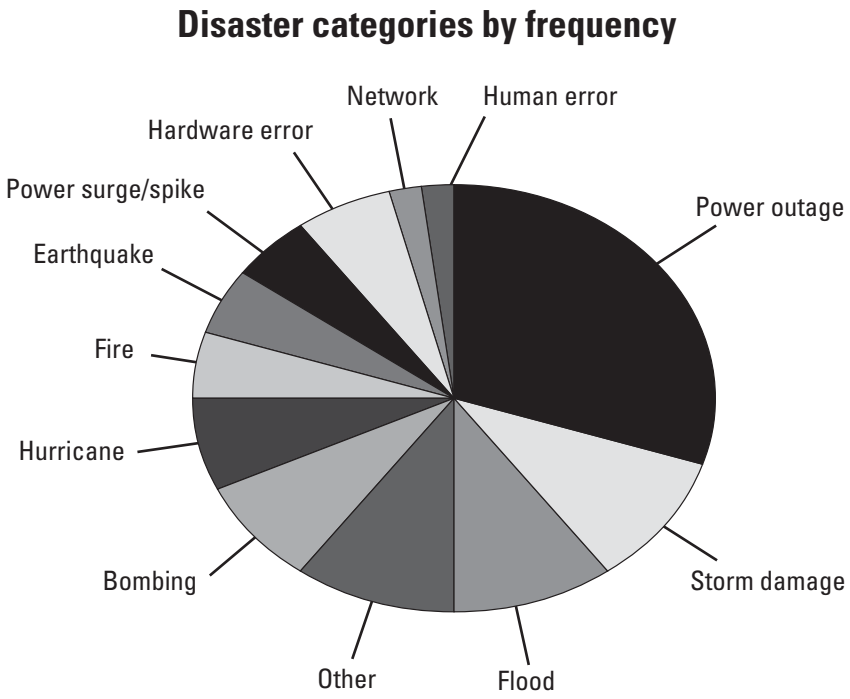

Figure 1.

Source: © Contingency Planning Research, a division of Eagle Rock Alliance, West Orange, NJ, www.eaglerockalliance.com.

These statistics show that 80 percent of all downtime is caused either by hardware, operational failures or human error, but the impact to the business is no less damaging regardless of the cause.

The difference in how well a business fares when a disruptive event strikes is often determined by the viability of the business continuity plan. A business continuity plan, including disaster recovery, should focus on people, facilities, data, systems and processes. These plans define specific procedures on how a business will keep functioning after a disruptive event.

3 ANATOMY OF FAILURE

The first dimension of failure is its scope. The scope might range from impacting one application to an entire IT environment, or from a single user to an entire region.

Risk of application and system failures can be mitigated locally, within existing data centers, with high availability systems and redundant platforms. However, for building, site and regional outages, companies should adopt alternate facility recovery techniques.

Planning for a single site failure requires an alternate facility and a regional disaster requires a geographically dispersed, alternate facility. For example, a data center in San Francisco, California that has the potential to be affected by an earthquake should have an alternate facility located outside of the fault zone. Secondly, what is often ignored is the company's most valuable asset, its employees and how they may be affected by the disaster. Productivity is strongly affected by lack of workplace resources; access to personal computers, telephone service, remote accessibility as well as emotional impacts. This was brought to light following the September 11 attack on the World Trade Center, where some companies were even forced to rent entire hotels in order to office their employees.

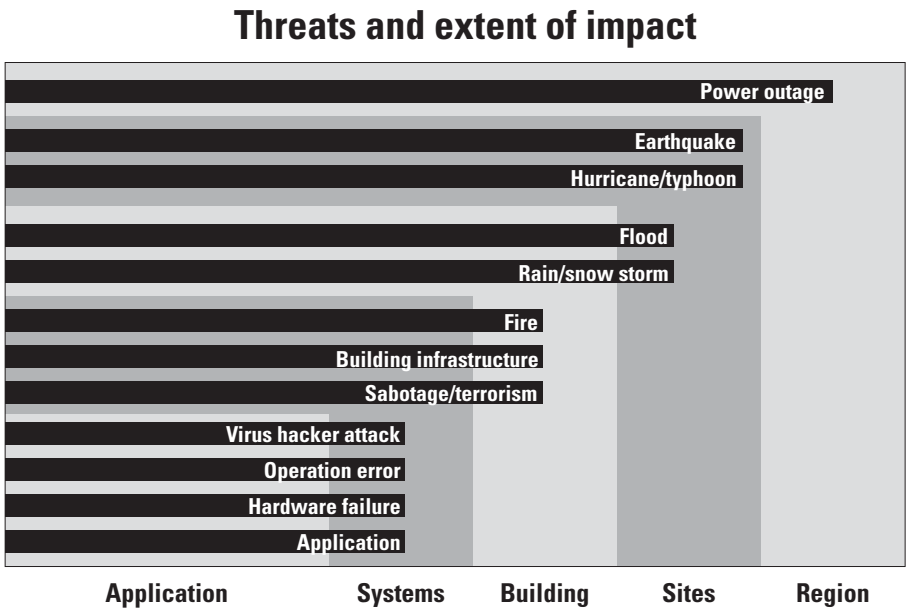

Figure 2.

Source: © Contingency Planning Research, a division of Eagle Rock Alliance, West Orange, NJ, www.eaglerockalliance.com.

4 COST OF FAILURE

The second dimension of IT failure is the cost of application outages. A report by Contingency Planning Research addressing the financial impact of application outages shows that outage costs can vary considerably by industry and application. The bottom line is, any outage can have a significant negative impact on your business.

Large cost associated with application outage indicates the significance it has to your business. Your application recovery plan should include not only the data, but the software as well. In many cases, application software can be restored from backups. If the software needs to be replaced, however, the amount of customization the application has undergone has to be considered. Customized software cannot be replaced "off-the-shelf." Operating systems and other software should be viewed in similar light. License keys, for accessing application software, should be obtained prior to a recovery scenario.

"Best practices" indicate companies should understand the criticality of their applications and data and are crucial when designing a business continuity solution. Applications that are less critical, or have data that can be easily recreated, will have a different design than one that requires little or no downtime. The more significant the application, the better protection it requires and the more costly the solution may be.

Financial impact of system failure		
Application	**Industry**	**Hourly cost**
Brokerage operations	Finance	$6.45 million
Credit card sales authorizations	Finance	$2.6 million
Pay-per-view	Media	$150,000
Home shopping (TV)	Retail	$113,000
Catalog sales	Retail	$90,000
Airline reservations	Transportation	$89,500
Tele-ticket sales	Media	$69,000
Package shipping	Transportation	$28,000
ATM fees	Finance	$14,500

Table 1. Hourly cost of application outage varies by industry.

Source: © Contingency Planning Research, a division of Eagle Rock Alliance, West Orange, NJ, www.eaglerockalliance.com.

5 BUSINESS CONTINUITY VERSUS DISASTER RECOVERY

While some people may think of business continuity and disaster recovery as synonymous, they are not. The ability to recover from a disaster is the result of a sound business continuity plan. Some companies make the mistake in assuming their disaster recovery plan is their business continuity plan. Disaster recovery, however, is only a component of the business continuity plan.

Disaster recovery is defined as the ability to restore critical business systems at time of disaster. Business continuity, on the other hand, is the ability to continue delivery of service in the event of any unplanned disruption. A comprehensive business continuity plan forces a company to look at its enterprise and identify the following:

> What are the critical business functions?
> Have the risks associated with these functions been quantified?
> What is the financial impact if these functions are lost?
> Have processes and procedures been developed to facilitate avoidance or mitigation of the risks?
> Has the plan been agreed to, and implemented at all levels of the organization?

Business continuity planning covers the full scope by determining the spectrum of business risks and planning ways to try to avoid them. It addresses continuance of business functions during recovery and, ultimately, full restoration of the enterprise following a disaster.

6 BUSINESS CONTINUITY PLANNING: THE BIG PICTURE

Business continuity planning must account for people, facilities, data, systems and processes. For any business continuity plan (BCP) to succeed, the plan must be bought into and brought into every level of the company from the CEO on down.

If an organization has the in-house expertise, a BCP can be handled internally. If not, it's a good idea to contract externally with experienced planners who can examine your environment from an objective point of view.

The BCP process should begin with a thorough analysis of systems, applications and processes. Secondly, the measurement of the financial impact of the major business groups and applications need to be prioritized by criticality. This analysis will help determine the recovery time objectives (the amount of time a company can be without their critical business functions) that support the organization's recovery strategies.

A successful BCP requires:

> Executive management commitment to project implementation
> Business continuity assessment
> Technology and business processes
> Business impact analysis
> Risk analysis and reduction
> Assessment of current threats, assets and alternatives
> Measurement of operational, financial, legal and regulatory impacts
> Planning
> Assessment of required scope
> Implementation of solutions that deploy required resources to continue business functions
> Development and documentation of plan
> Awareness, training, implementation and continual testing and updating

7 BUSINESS IMPACT ANALYSIS: ASSESSING RISKS AND PRIORITIES

The business impact analysis (BIA) is a critical contributor to the business continuity plan. It is the process that helps quantify and prioritize requirements for the business continuity strategy. The BIA assesses the risks for equipment, applications and data, and establishes the recovery time objectives. Some sample questions that the BIA will pose are:

> Which business functions are critical?
> What is the cost per hour of losing a specific function?
> Does the organization rely heavily on e-commerce?
> What is the current state of readiness?
> How quickly and in what order must systems be restored?

Answering these questions will help an organization determine what processes and applications are critical, vital or non-critical and can be recovered without further threatening the company's ability to do business.

In defining priorities, as with all of business continuity planning, executive involvement is absolutely critical — not only because of the impact on costs, but to secure the buy-in of the entire company at all levels and disciplines.

7.1 CREATING A RECOVERY HIERARCHY

As the BIA helps prioritize applications, data, functions and processes, a recovery hierarchy will identify and rank applications and supporting systems that require:

> Immediate recovery
> Up to four hour recovery
> Same day recovery
> Up to 24 hour recovery
> Up to 72 hour recovery
> Seventy-two hours or greater recovery

Classifications help sort data into the appropriate categories:

Critical: Systems, applications and data critical to the company's ability to function, used in key business processes or necessary for legal reasons.

Vital: This refers to the set of data and/or applications a company can function without for a short period of time. This data is used in standard business process that represents a significant investment of the company's resources.

Non-critical: Data that can be reconstructed at a minimal cost. It is data that has already been copied and has low security requirements.

After the classification of the data has occurred, the recovery hierarchy will map out the order in which the systems need to be recovered. In today's world of e-everything, some applications and data must always be available. High availability requirements are more complex, entail more resources and are, therefore, more expensive. In general, the more immediate the requirement for data availability, the greater the cost.

8 ELEMENTS OF RECOVERY

If resumption of business processing can be 48 hours or more, a cold site may be adequate for recovery. In this case, equipment is installed and configured in the cold site only after a recovery plan is invoked. While they are significantly less expensive to maintain than hot sites, colds sites may require very time-sensitive equipment delivery agreements with major vendors and suppliers.

The most common recovery approach is restoring the environment using tape media that has been shipped to an alternate location. Organizations can also procure equipment when needed on a quick-ship basis, or can subscribe to a commercial hot site recovery vendor.

A more advanced recovery process would be to connect two tape libraries together through a remote electronic storage system (RESS) or electronic remote vaulting. Electronic vaulting creates backup tapes either directly from primary disk or primary tape to a tape library at a remote site. In the event of disruption, tape copies of data are readily available at the recovery site, eliminating the need to ship tapes from a third-party storage facility.

Very critical applications may require either an internal hot site or an outsourced hot site from a commercial provider, complete with power, equipment and communication facilities. To do this, some companies use secondary, mirrored facilities that are identical in many respects to the primary data center. Data is electronically moved from the primary site to a redundant one via hardware and software tools. In some cases, the secondary facilities host active applications and can act as a load-sharing site.

For greater protection of data using disk solutions, mirroring or shadowing may be required. Mirroring maintains a replica of databases and file systems by applying changes at the secondary site in lock step with, or synchronous to, changes at the primary site. The I/O operation is not complete until both the primary and secondary copies are updated.

"Backup is important, recovery is mission-critical."

Data Security — The Rules are Changing,
Fred Moore, Horison, Inc., September 27, 2001

Shadowing is an asynchronous process that maintains a replica of databases and file systems by capturing changes and applying them, based on user defined policies, at the recovery site. In asynchronous replication, the I/O operation is released as soon as the primary site cache confirms acceptance to the host. The secondary site is updated asynchronously (at a later time) and will therefore always have some degree of aged data.

Mirroring may require significantly more bandwidth than shadowing. Too little bandwidth or high latencies will degrade production system performance, or even hang certain applications. Because of this latency, synchronous hardware mirroring has distance limitations. Shadowing, on the other hand, allows the two sites to be a virtually unlimited distance from one another, but will always have some degree of data loss. The trick is to know which tool is right for the situation.

8.1 THE ROLE OF DISK

High-impact, mission-critical applications and databases requiring instant failover benefit from real-time electronic mirroring. Disk subsystems such as the V-Series Shared Virtual Array® (SVA™) using Peer-to-Peer Remote Copy (PPRC), support such mission-critical requirements by simplifying storage administration across the enterprise. With its unique ability to mirror compressed data and minimize overhead data such as free space requirements, the SVA system may reduce network requirements. This capability, in some cases, can also increase operational distances of a mirrored site.

Integrated in mainframe systems, virtual disk solutions can reduce production downtime for backups and provide the fastest backup and recovery without requiring any additional disk space. These solutions minimize business interruption using SnapShot software to create instantaneous copies, which can be restored almost immediately.

8.2 REMOTE TAPE SOLUTIONS

Automated tape solutions are by far the most cost-effective method of storing large quantities of data across a broad geographic area. Both removable and portable, tape solutions are available for every level of need from the low-end to fully mirrored tape libraries with virtually unlimited capacity. Tape solutions can also exploit virtual storage management solutions, be used to create virtual tape drives (saves money), increase speed of backups/restores, and simplify overall data management. Automated, virtualized tape solutions not only get far more storage from the same physical space, but the library can be connected to handle remote electronic storage system (RESS)/electronic remote vaulting (ERV).

For applications with lower business impact, implementing a solution such as StorageTek Automated Cartridge Systems (ACS) for data redundancy addresses both timeliness and budget. High-performance, highly reliable tape devices, such as the T9840 and T9940 tape drives, minimize the data recovery times when a recovery plan is invoked.

The ability to migrate data from disk to tape automatically also allows for cost-effective, multi-generational backups. With disk, errors or corruption problems in the primary data are propagated to the remote location. As a result, data may have to be restored from an older generation to locate a “clean” copy of the data. With tape, multi-generational copies are inexpensive and quickly searched and retrieved.

8.3 SIMPLIFY WITH SOFTWARE

Software is a key factor in the ability to move files quickly and recover even the largest data files in minutes. For example, Application Storage Manager® (ASM) software exploits storage virtualization and automates data management and retrieval across the storage hierarchy via user-defined data policies. The data policies can be specific to individual applications or even to groups of files that are sharing a common storage system consisting of disk and tape. The data is fully accessible from any tier of storage at any time. The benefit of ASM is to offload data from the disk cache to tape allowing companies to balance cost, performance and capacity to lower the total cost of ownership. Multiple copies can be concurrently created for the main location, "cave" and/or remote location.

In addition to archiving the files, ASM software also archives the directory and file location. The media is labeled using American National Standards Institute (ANSI) standard volume labels to ensure that access is maintained. Data is written in standard TAR format allowing for recovery with or without ASM on the UNIX platform. Recovery on the Windows or OS/390 platform does require ASM for Windows or ASM for OS/390 respectively.

9 CHOOSE A COMPREHENSIVE AND EXPERIENCED STORAGE VENDOR

Many storage vendors offer a part or parts of a disaster recovery solution. But piecemeal solutions typically buy more frustration and cost more than one designed by a proven provider of coherent business continuance storage plans, products and services.

Look for a vendor who specifically provides professional business continuity auditing and planning services, as well as complete solutions, implementation and support to realize the plan and refresh it as needed. A strong vendor will offer experience and consulting services, including certified disaster recovery planners, to help you assess risks and analyze their business impacts.

The right storage solution partner can guide you in developing detailed business continuance, risk management and risk mitigation requirements using proven methodologies including business impact analysis. They can help you consider all business interruption risks, from local hardware and software failures to regional interruptions. They can help establish policies and procedures and a management process to execute the plan. And, in addition to designing, scaling and implementing a viable, business continuity solution based on specific recovery needs, they can provide crucial back-end support to maintain and service the solution.

It is also important to choose a vendor who has a breadth of products with a technology roadmap, solid third-party partnerships and a large installed base. Such a vendor will offer, and be able to maximize, a full scope of seamlessly integrated disaster recovery and storage products including scalable disk, tape, virtual storage solutions, SAN solutions, software and global professional services. With an experienced vendor, companies can leverage virtual technologies and exploit the benefits of virtually instantaneous copies as well as reduce costs with solutions such as transporting data over TCP/IP.

10 IS YOUR BUSINESS PREPARED?

In business, the threat of a disastrous situation is real. Interruptions to business operations can be sudden, dramatic and widespread. They can come from anywhere — natural forces, human or equipment error. With our growing reliance on data and e-business, the importance of developing, implementing and maintaining effective business continuity and disaster recovery plans becomes even clearer.

The optimal solution should consider both the immediate and future circumstances and problems your business faces. And your recovery platforms should not only address those, but also help you stay competitive by positioning you to take advantage of new capabilities as they are delivered.

Once you have a viable business continuance plan, test it, practice it, refine it and maintain it. But don't wait. It is never too early to start planning for success. If disaster strikes and you are not ready, it could be too late.

11 DISASTER RECOVERY GLOSSARY

Hot site

A remote facility used to house a company's business information and computer systems should the primary area of operation/data center become unavailable. There are two types of hot sites: internal and outsourced.

Internal hot site

An internal hot site is where the business selects and uses its own resources. Since the resource is "owned" by the organization, it can engineer the site to be more responsive and robust than any other solution. An internal hot site allows an organization to control its recovery assets and can be tested and verified frequently.

Outsourced hot site

An outsourced hot site is where a company contracts with a provider for either fixed or mobile alternate location, and can contract for business continuity, disaster recovery and other services. This model shares the resources, as well as the risk of availability with other companies.

"Cold" site

Typically a vacant room with enough space and cabling to allow it to be set up with equipment and personnel on short notice. Since this solution requires starting "cold," the set-up process could take anywhere from one to two weeks or even longer.

Tape vaulting

Physically moving tapes to an offsite location. Sometimes referred to as "the pickup truck access method," this is when companies choose to ship their backup tapes offsite to a vault or site of their choice.

Reciprocal agreements

Agreements made between companies to house each other's data. They often involve legal complexities and space in each other's data centers. Depending on proximity, both sites could be at risk should a regional disaster occur.

ABOUT STORAGETEK®

Storage Technology Corporation (NYSE: STK), a $2 billion worldwide company with headquarters in Louisville, CO, has been delivering a broad range of storage management solutions designed for IT professionals for over 30 years. StorageTek offers solutions that are easy to manage, integrate well with existing infrastructures and allow universal access to data across servers, media types and storage networks. StorageTek's practical and safe storage solutions for tape automation, disk storage systems and storage integration, coupled with a global services network, provide IT professionals with confidence and know-how to manage their entire storage management ecosystem today and in the future.

StorageTek products are available through a worldwide network. For more information, visit www.storagetek.com, or call 1.800.275.4785 or 01.303.673.2800.

WORLD HEADQUARTERS

Storage Technology Corporation
One StorageTek Drive
Louisville, Colorado 80028 USA
1.800.877.9220 or 01.303.673.5151

MZ 9149 F 04/04