IBM Solutions
Point of view
September 2006

Panic slowly.

Integrated disaster response and built-in business continuity

Contents

"We've got a plan!" Many a CIO has come to rue making such a blanket statement to a CEO regarding the company's disaster preparedness. A decade of regional calamities has shown that traditional approaches to disaster planning have failed to keep organizations operational. IT-focused recovery plans can leave the overall organization in the lurch because they often don't address such business issues as handling a disaster that is regional in nature; employee availability; communications; travel and transportation; and data location and availability. But an integrated business continuity and resilience plan can take some of the pressure off CIOs by reducing the business impacts of a disruptive event, speeding recovery times and delivering value to the organization—even if a disaster never strikes.

How much is your reputation worth?

It seems as though you can't turn on your TV or launch your browser these days without learning of a natural disaster, terrorist plot or hazardous materials accident. Organizations in different parts of the globe may face different threats—in the Americas, catastrophic weather is a concern; in Asia, pandemics and blackouts may be paramount; in other parts of the world, there is significant civil unrest. Regardless of where you are located, chances are your disaster risk levels have increased in recent years. Shifting business models—driven by increased customer expectations for 24x7 access to your services, changing regulatory requirements and new networking technologies—mean that business continuity is increasingly important. It's easy to be left behind—particularly if your infrastructure is not designed to support a resilient organization.

The last thing you want to do is put your boss in the hot seat because of an IT failure.

Highlights

It's also true that downtime costs you more than it used to. The average number of downtime hours experienced each year ranges from about 300 in logistics to nearly 1,200 in financial services, with the bulk coming from outages. Downtime costs financial companies as much as 16 percent of their revenue, annually.[1] And that's not even counting the damage to your brand, especially if your organization depends on the Internet for business. Nor does it account for regulatory penalties. Or shareholder flight—a study conducted by IBM Research finds that companies can see a 10 percent reduction in shareholder value from events resulting in reporting and processing errors, application failures or supply chain disruptions. No CEO or public administrator wants to be on the front lines of such a revenue and public relations catastrophe, and no CIO wants to put a boss in that position.

CIO disaster planning checklist:

- ✓ *Reduce overall risk*
- ✓ *Maintain a current, tested plan*
- ✓ *Allay user and investor concerns*
- ✓ *Improve day-to-day service levels*
- ✓ *Comply with regulations*
- ✓ *Respond rapidly if a disaster occurs*

In addition to allaying your CEO's and your shareholders' (or constituents') concerns about your ability to protect the business operations during a disaster, you now have the opportunity to deliver an even more compelling message. A good recovery and resilience plan can actually help your organization perform better day to day. It can also help with overall risk management and audit readiness. This paper offers support to the CIO confronted with increased responsibility for the business impacts of systems downtime. It helps you assess your own preparedness, examines new approaches and technologies, and explores the business justification for investing in disaster preparedness and organizational resilience.

Highlights

The basics: What is business continuity and resilience?

Business continuity and resilience is a combination of proactive and reactive strategies that keep your critical business processes available, practically without interruption — while improving your operational efficiency. Availability solutions can help reduce the chances that a systems failure will force you to declare a disaster. And disaster recovery solutions can bring your business processes back online faster if a serious disruption does occur. In our view, business continuity planning is best broken down into four project areas.

Most comprehensive continuity plans combine availability and recovery solutions.

***Availability** solutions keep your critical business and IT processes available and resilient in the face of uncertainty.*

***Recovery** solutions help you restore business processes, systems, networks and data if the worst really does happen.*

***Backup and restore** solutions support high availability and make recovery easier by meeting your day-to-day needs for data continuity and protection, including recovery time and recovery point objectives.*

***Crisis management** solutions provide crisis response planning as well as onsite expertise and direction if a disaster does occur, managing employees, communications and logistics.*

In IBM’s view, effective disaster planning will build an increased capacity for availability, recovery, backup and crisis response into the organization at all levels, from facilities to management and planning. Typically built on open architectures, infrastructures designed for business continuity create resilient organizations that can adapt and respond to change — including growth opportunities.

Highlights

Hindsight is 20/20

Many IT departments have some kind of disaster plan in place. However, as recent headlines have demonstrated, the scale and business impact of a disaster in today's interconnected world have ambushed many a CIO. Typically, a disaster plan will establish a recovery point and a recovery time objective for restoring infrastructure operations, while leaving many other business-critical processes unaddressed. Such as how will your employees get to work? Will they be able to maintain focus if their families' health or safety is threatened? What happens if your backup tapes are damaged? What if power is not restored within 24 hours? What if your operations are unaffected, but your partners and suppliers are unable to deliver what your business needs?

Most IT disaster plans don't address a regional emergency–or the business impacts of sustained downtime.

IBM's global crisis management team has been on site at more than 70 disasters in the past decade. We've seen that the typical IT plan for infrastructure recovery only scratches the surface of the issues that bring organizations down. The most common gaps were employee unavailability, communications breakdowns, extended power outages, damaged backup tapes, and travel and transportation restrictions. Many companies and agencies failed to take into account a disaster that was regional in nature and believed that, as long as they had multiple facilities and local cell phones, they would be able to maintain business operations. Here are some of the lessons we've learned:

- *Personnel issues will be your primary concern–your plans should take into account your employees' personal needs.*
- *Power failures take down telecommunications–network providers and individual phone batteries require electricity.*
- *Travel and transportation will be restricted–plan for disabled vehicles, limited rental car availability and dwindling fuel supplies.*

Highlights

Business continuity is not just an IT function–it's a core component of your organization's culture.

- *Critical facilities should not be located in close proximity.*
- *Resources should be staged in safe areas–switching equipment, generators and fuel tanks should be located above flood levels.*
- *Data management challenges will arise–backup systems should not require physical connectivity to your infrastructure.*
- *Insurance coverage is often inadequate–understand your coverage before disaster strikes, and document activities for adjusters.*
- *Hardware may be damaged–develop and test a plan for replacing equipment and for disposing of unusable devices.*

Cleaning up after Katrina

A leading American manufacturer of household cleaning technology is headquartered in New Orleans, with its main manufacturing facility in southern Mississippi. Prior to Hurricane Katrina, it considered itself well-prepared for disaster, and in fact it had a plan that was more complete than most. It was operating in a distributed environment and storing backup tapes offsite. It also had planned for call center partners to take over communications, and for a local hosting partner to manage Web and retail recovery.

Even so, the company drew some critical lessons from the Katrina disaster. The company saved its business operations by moving key employees and their families out of the disaster area, so that they would be free to focus on restoring the business without the distraction of worrying about the safety of loved ones. It became clear that business continuity was not an IT function, but rather a mindset and the result of an enterprise culture. The company also learned that political relationships are critical, and that business continuity planning must include and involve call center, supply chain and hosting partners.

On the IT side, the company learned that a simple shutdown and restart of operations was not enough to make the business operational. In a regional disaster, tape-based backup was not as reliable. In terms of restoration, it was reminded that the network is a critical system, and e-mail is the first application that needs to be recovered. One key lesson was that a flexible architecture could decrease recovery times and costs.

Highlights

A proactive, comprehensive approach helps you protect your business. Not just your infrastructure.

A proactive approach

As you create or update your business continuity plans, you'll need to consider a number of areas that extend beyond the strict province of IT. An effective business continuity plan calls for an interdisciplinary, organization-wide approach. It should take into account the potential for a disaster to strike across an entire region, bringing down external infrastructures and supply chains. And it should incorporate both proactive and reactive elements. Many components, such as meeting service levels, data continuity and regulatory compliance, deliver additional business benefits. In our view, each aspect of such a comprehensive program complements the others; how much you need of each will depend on your existing state of readiness, your industry and your overall business goals.

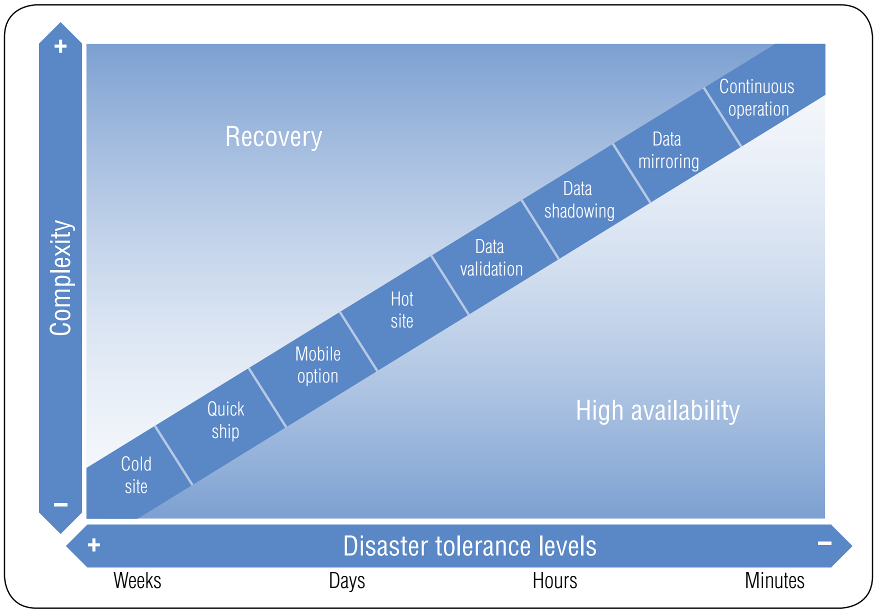

Figure 1. An effective continuity program must address the needs of all layers of your business.

Highlights

The keys, as always, are to plan ahead, and plan well.

Regardless of your particular business continuity and disaster recovery needs, you'll need to think proactively about your strategy. You don't want to be in the middle of an earthquake when you learn that all of your data centers are vulnerable. There is no one-size-fits-all solution—an approach based on meeting your business priorities will have your own unique stamp. The most successful programs will probably be a hybrid of lessons learned from recent disasters and careful planning. The key is to base your approach on an inventory of your prioritized business processes, so you can ensure that the organization itself recovers—and not just the infrastructure.

Banking on high availability

Business need

A leading Spanish bank wanted to protect its position in the marketplace by managing the overall risks associated with unplanned system outages—risks such as customer dissatisfaction and regulatory penalties. It also wanted to reduce IT costs and improve security at its two data centers.

Solution

The bank implemented a business continuity and recovery solution based on a highly available and automated information technology infrastructure. The solution included hardware, software and services and provides automated recovery policies for planned and unplanned outages—including automated switching between data centers, data sharing, workload balancing, automated fail-over support, performance management and dashboard access.

Benefits

- *Reduced the time needed to switch between data centers from days to under two hours*
- *Reduced risk of lost revenue*
- *Decreased risk of regulatory penalties*
- *Reduced requirement for capital reserves, per Basel II, freeing up operating capital*

Highlights

You're probably already investing in technology you could leverage to make your organization more resilient.

Using technology innovation for built-in business continuity

Many of the technologies you have already installed or may be considering as you push to make your overall operations more efficient will also, with appropriate forethought and design, support business continuity and disaster recovery. For example, network resource virtualization, which automatically assigns and reassigns resources based on network loads, can help you make the most of your existing infrastructure investments while supporting flexibility. Autonomic computing capabilities scan networks, monitoring for problems and breaches, and automatically fix many problems as they arise. They can make infrastructures and applications more resilient and reliable, helping maintain service levels while reducing the load on IT staff.

Parallel computing, by adding more processing power to your network, is another technology that can increase availability and support intensive data-crunching needs. Regardless of your vulnerability to a disaster, supplementing traditional, tape-based systems with digital backup systems and storage area networks that do not need a physical connection to your infrastructure can be a good business move.

Managed hosting opportunities provide another way for companies to leverage advances in networking technologies. By outsourcing key business continuity, data center, backup and recovery operations to qualified providers, organizations can focus resources on their core business.

Highlights

Steps toward an integrated continuity plan

Although contemplating a comprehensive approach to business continuity may seem overwhelming, you can build a resilient organization incrementally. Begin with a comprehensive assessment of where you are and where you want to go. You'll need to measure your own plans and capabilities against some of the gaps and shortfalls enumerated at the beginning of this paper, including the need to plan for a disaster that might be regional in scope.

Start at the beginning: assess your disaster tolerance against your readiness levels.

With those gaps in mind, identify the business processes without which your enterprise, customers and partners couldn't survive. Which of those processes will you need to restore first? What steps can you take in the meantime to reduce your vulnerability to disaster, make your daily processes more efficient and deliver an ongoing return on your business continuity investment?

After you've assessed your readiness in the areas on which you want to focus, you'll need to weigh both the availability and the recovery sides of the equation. Consider the value of open source applications and systems in helping you build a resilient, scalable environment that can respond robustly to a variety of business challenges and disruptive events. Evaluate managed hosting and data center options to keep your costs of ownership low and your innovation quotient high. Investigate electronic data management options as a way to protect both your daily data access and your restoration needs.

Next, develop your continuity plan and implement the procedures that support it. Validate your program—repeatedly—through scenario testing. When your plan is deployed and your networks are integrated, consider redirecting resources toward differentiating business activities by outsourcing the management of your business continuity program and service levels.

Highlights

What to look for in a business continuity solutions provider

The degree to which you turn to outside providers for help developing your business continuity solution will depend on your goals. Because of the multifaceted nature of business continuity and disaster recovery planning, many companies favor a solutions-oriented approach to avoid the gaps, integration headaches and costs associated with purchasing hardware, software and services separately. Even if you decide to create and implement your plan inhouse, you may still find it valuable to consult with a solutions provider upfront to identify and prioritize critical business processes and to verify that you have addressed the many facets of an effective recovery plan.

An experienced solutions provider can help you avoid common pitfalls in disaster planning.

As you search for a qualified provider, you may want to emphasize the following:

- *Does the provider have experience in assessing and planning for the risk of a regional disaster?*
- *Does the provider have established methodologies and documented best practices?*
- *How innovative is the company—what is its level of expertise regarding systems and technologies that support continuity, and how well does it understand your own needs for business innovation?*
- *Does the provider have comprehensive IT capabilities and the ability to tailor a solution that combines hardware, software and services?*

Highlights

Once you know your risk tolerance and readiness, you can tailor a solution that meets your needs.

- *Does the provider's solution portfolio include policy-based automation, automatic fail-overs that can be exploited for both planned and unplanned events, and workload balancing?*
- *Will the provider work with you to develop a solution that delivers what you need—and no more than you need?*
- *How well does the provider understand your particular industry and the local, regional and global standards and regulations that apply?*
- *Is the provider itself required to demonstrate audit-readiness and comply with extensive regulations (for example, a public company may have more direct experience with these issues than a private one)?*

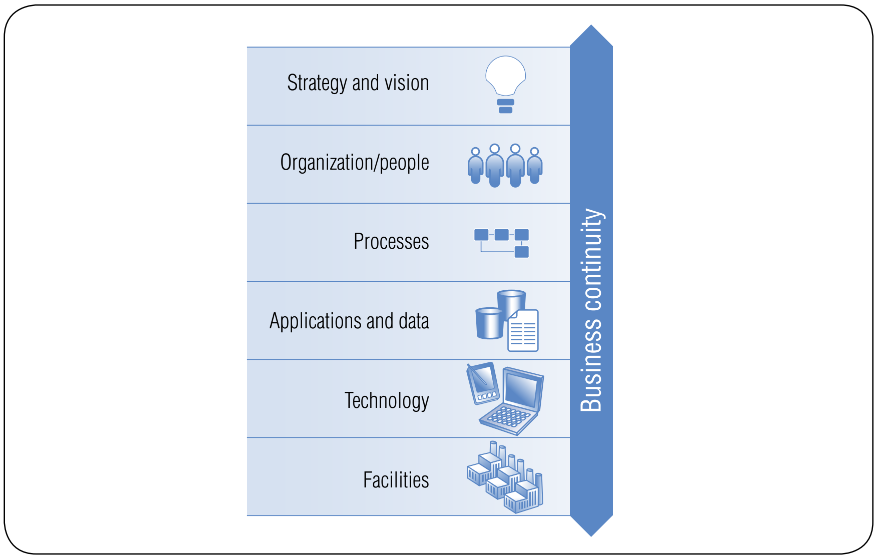

Figure 2. There is no one-size-fits-all approach to disaster planning and business continuity. A variety of solutions can be configured to match your company's particular requirements, priorities, risk tolerance levels and preferences.

Highlights

- *Does the provider have a truly global presence and delivery capability?*
- *What is the provider's track record in recovery and crisis response?*
- *How much on-the-ground, on-site crisis management and response experience does the provider have?*

Justifying your investment in business continuity

Can you afford to let your business down?

Recent disasters, regulatory requirements, customer and partner expectations, the realities of doing business online—all highlight the need to present corporate management with the business case for doing the job right. There are practically as many drivers for investing in comprehensive recovery plans as there are businesses. High availability is a cross-industry concern; from government agencies to financial services providers, to online retailers and to data-intensive biotechnology companies—systems and data need to be continuously available. The best way to ensure recoverability and data continuity is to design networks, processes, policies, applications and data management systems that support high availability from the beginning.

Highly resilient and available businesses are built on open architectures, making them more scalable and responsive to change—which aids in a disaster response but also makes the organization more resilient in the event of any change in marketplace conditions, including new opportunities and competitive positioning. Organizations recognized for maintaining strong service levels, data continuity and management procedures in the event of a crisis are more likely to win the approval of auditors, shareholders or constituents.

For these reasons, business continuity and resilience has moved beyond serving as an insurance policy against the unthinkable. However, if the unthinkable—which seems increasingly more thinkable these days—does occur, a well-considered disaster recovery plan will help you avoid the business impacts of downtime. Few businesses can sustain the losses associated with downtime and remain competitive. Make sure yours is one of them.

For more information

To learn more about IBM's views and capabilities regarding business continuity and resilience solutions, contact your IBM representative or visit:

ibm.com/solutions/itsolutions

© Copyright IBM Corporation 2006

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
09-06
All Rights Reserved

IBM and the IBM logo are trademarks of International Business Machines Corporation in the United States, other countries or both.

Other company, product and service names may be trademarks or service marks of others.

References to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.

[1] Dearborn, Rob, *et al.*, "The Costs of Enterprise Downtime: North American Vertical Markets 2005," Infonetics Research, January 2005, p. 79.