

# Business Continuity: New risks, new imperatives and a new approach



**Thought  
Leadership**

## Introduction

*“The wonder of the Web is that the customer knows about IT problems the same time you do. There’s no camouflage.”*

*– Senior VP of electronic brokerage technology<sup>1</sup>*

Your data center is performing flawlessly, your network is up and your call center is operating normally. But over the last 24 hours, your company lost millions of dollars of market capitalization. A degradation in performance of a Web server, coupled with staff shortages, led to a complete outage of your online business.

Could this disaster have been prevented? Until recently, classic recovery planning focused on how to restore centralized data centers in the event of a natural or man-made catastrophe. It did not address the need for continuous operation of key business processes. While traditional measures remain important, they are far from adequate for distributed computing environments. The requirements for continuous operations in an e-business, Web-speed world are even more complex and challenging.





## Trends and directions—beyond disaster recovery

When disaster recovery emerged as a formal discipline and a commercial business in the 1980s, the focus was on protecting the data center—the heart of a company’s heavily centralized IT structure. This model began to shift in the early 1990s to distributed computing and client/server technology. At the same time, information technology became embedded in the fabric of virtually every aspect of a business. Computing was no longer something done in the background. Instead, critical business data could be found across the enterprise—on desktop PCs and departmental local area networks, as well as in the data center.

This evolution continues today. Key business initiatives such as enterprise resource planning (ERP), supply chain management, customer relationship management and e-business have all made continuous, ubiquitous access to information crucial to an organization. This means business can no longer function without information technology: data, software, hardware, networks, call centers—even laptop computers.

A company that sells products on the Web, for example, or supports customers with an around-the-clock call center, must be operational 24 hours a day, 7 days a week—or customers will go elsewhere. An enterprise that uses e-business to acquire and distribute parts and products is not only dependent on its own technology but that of its suppliers. As a result, protecting critical business processes, with all their complex interdependencies, has become as important as safeguarding data itself.

The goal for companies with no business tolerance for downtime is to achieve a *state of business continuity*, where critical systems and networks are continuously available, no matter what happens. This means thinking proactively: engineering availability, security and reliability into business processes from the outset—not retrofitting a disaster recovery plan to accommodate ongoing business continuity requirements.



### Business continuity: Whose responsibility is it?

Many senior executives and business managers consider business continuity the responsibility of the IT department. However, it is no longer sufficient or practical to vest the responsibility exclusively in one group. Web-based and distributed computing have made business processes too complex and decentralized. What's more, a company's reputation, customer base and, of course, revenue and profits are at stake. All executives, managers and employees must therefore participate in the development, implementation and ongoing support of continuity assessment and planning.

The same information technology driving new sources of competitive advantage has also created new expectations and vulnerabilities. On the Web, companies have the potential to deliver immediate satisfaction—or *dissatisfaction*—to millions of people. Within ERP and supply chain environments, organizations can reap the rewards of improved efficiencies, or feel the impact of a disruption anywhere within their integrated processes.

With serious business interruption now measured in minutes rather than hours, even success can bring about a business disaster. Web companies today worry more about their ability to handle

unexpected peaks in customer traffic than about fires or floods—and for good reason. For example, an infrastructure that cannot accommodate a sudden 200 percent increase in Web site traffic generated by a successful advertising campaign can result in missed opportunities, reduced revenues, and a tarnished brand image.

Because electronic transactions and communications take place so quickly, the amount of work and business lost in an hour far exceeds the toll of previous decades. According to a report published by Strategic Research Corporation, a Santa Barbara, California, market research and consulting firm<sup>2</sup>, the financial impact of a major system outage can be enormous: US\$6.5 million per hour in the case of a brokerage operation; US\$2.6 million per hour for a credit-card sales authorization system; or a mere US\$14,500 per hour in automated teller machine (ATM) fees if an ATM system is offline.

Even what was once considered a “minor” problem—a faulty hard drive or a software glitch—can cause the same level of loss as a power outage or a flooded data center if a critical business process is affected. For example, the New York-based research firm FIND/SVP calculates the average

financial loss per hour of disk array downtime at US\$29,301 in the securities industry, US\$26,761 for manufacturing, US\$17,093 for banking and US\$9,435 for transportation.<sup>3</sup> More difficult to calculate are the intangible damages a company can suffer: lower morale and productivity, increased employee stress, delays in key project timelines, diverted resources, regulatory scrutiny and a tainted public image.

In this climate, executives responsible for company performance now find their personal reputations at risk. Routinely, companies that suffer online business disruptions for any reason make headlines the next day, with individuals singled out by the press. Moreover, corporate directors and officers

can be liable for the consequences of business interruption or loss of business-critical information. Most large companies stipulate in their contracts that suppliers must deliver services or products under any circumstances. What's more, adequate protection of data may be required by law, particularly for a public company, financial institution, utility, health care organization or government agency.

Together, these factors make business continuity the shared responsibility of an organization's entire senior management, from the CEO to line-of-business executives in charge of crucial business processes. Although IT remains central to the business continuity formula, IT management alone cannot determine which processes are critical to the business and how much the company should pay to protect those resources.

---

### **The Internet brings new risks**

*A recent IBM survey of 226 business recovery corporate managers revealed that only eight percent of Internet businesses are prepared for a computer system disaster. Yet doing business online means exposing many business-critical applications to a host of new risks.*

*While the Internet creates tremendous opportunity for competitive advantage, it can also give partners, suppliers, customers, employees and hackers increased access to corporate IT infrastructures. Unintentional or malicious acts can result in a major IT disruption. Moreover, operating a Web*

*site generates organizational and system-related interdependencies that fall outside of a company's control—from Internet Service Providers (ISPs) and telecommunications carriers to the hundreds of millions of public network users.*

*Therefore, the greatest risk to a company's IT operations may no longer be a hurricane, a 100-year flood, a power outage or even a burst pipe. Planning for continuity in an e-business environment must address vulnerability to network attacks, hacker intrusions, viruses and spam, as well as ISP and telecommunication line failures.*



### Planning for business continuity: A proactive approach

Few organizations have the need or the resources to assure business continuity equally for every functional area. Therefore, any company that has implemented a single business continuity strategy for the entire organization is likely underprepared, or spending money unnecessarily.

The key to business continuity lies in understanding your business, determining which processes are critical to staying in that business, and identifying all the elements crucial to those processes. Specialized skills and knowledge, physical facilities, training and employee satisfaction—as well as information technology—should all be considered. By thoroughly analyzing these elements, you can accurately identify potential risks and make informed business decisions about accepting, mitigating or transferring those risks. Once you have developed a program for assuring that critical processes will be available around the clock, assume that it will fail—and commit to keeping your program current with business and technology infrastructure changes.

A fail-safe strategy assumes that no business continuity program can provide absolute protection from every type of damage—no matter how comprehensive your high-availability, redundancy, fault tolerance, clustering and mirroring strategies. Today,

the disasters most likely to bring your business to a halt are the result of human error or malice—the employee who accidentally deletes a crucial block of data; the disgruntled ex-employee seeking revenge by introducing a debilitating virus; the thief who steals vital trade secrets from your mainframe; or the hacker who invades your network. According to a joint study by the U.S. Federal Bureau of Investigation and the Computer Security Institute, the number and severity of successful corporate hacks is increasing dramatically—particularly intrusions by company insiders. In one study, 250 Fortune 1000 companies reported losses totaling US\$137 million in 1997—an increase of 37 percent over the previous year.<sup>4</sup>

Making an executive commitment to regularly testing, validating and refreshing your business continuity program can protect your company against perhaps the greatest risk of all—complacency. In the current environment of rapid business and technology change, even the smallest alteration to a critical application or system within your enterprise or supply chain can cause an unanticipated failure to your business continuity. Effective business protection planning addresses not only what you need today, but what you will need tomorrow and into the future.



## Do it in-house, or use a business continuity provider?

Highly successful companies recognize the value of a technology solutions provider that can help plan, implement and manage an ongoing business continuity program.

As client/server computing became more widespread in the early 1990s, and the price/performance ratio for computing and storage continued to improve, many companies implemented in-house data mirroring, redundant storage arrays and other high-availability techniques to create duplicate online or near-online copies of data.

Although these strategies can provide virtually continuous availability of data at very attractive price points, enterprises that test and validate their ability to recover from an outage have learned that business continuity encompasses many more challenges. To provide true continuity for critical business processes—not just critical data—companies using the in-house approach must also:

- Ensure that sufficient latent capacity will be immediately available to assure rapid failover and recovery
- Test capacity availability without disrupting ongoing operations
- Install redundant network capacity dedicated to business continuity
- House failover equipment in a separate location from the main production equipment and provide further redundancies, such as sourcing electrical supplies from different power grids
- Establish and maintain relationships with vendors to assure quick delivery of replacement PCs, network hardware, desks, chairs, telephones, etc., in the event of a facility-wide disaster
- Secure adequate funding from end-user departments to implement and maintain adequate critical business continuity protection
- Acquire, train and retain skilled personnel who can manage the complex interdependencies and specialized elements of business continuity
- Make adequate provisions for adding recovery support staff in the event of a regional or natural disaster.

Using a technology solution provider for part or all of these requirements can be attractive for companies that prefer to focus already scarce resources on driving revenue growth and increasing shareholder value. By establishing a long-term strategic relationship with a world-class services provider such as IBM Global Services, companies can gain a competitive advantage through a customized continuity plan, while avoiding the cost of keeping up with technology and training.

Engaging a business continuity provider enables these organizations to:

- Leverage the provider's extensive investments in the latest technology, continuous improvements to methodologies, and skilled people
- Benefit from the expertise gained in solving problems for a variety of clients with similar requirements
- Remove expensive, redundant technology assets from the balance sheet
- Use the provider's backup facilities and resources
- Take advantage of the provider's economies of scale on assets, resources and procurement to help enable a lower cost of operation and significantly less risk
- Concentrate on achieving core business growth objectives.



## Business continuity readiness

This simple self-audit can help you with the important task of assessing your company's business continuity readiness.

If you answer "No" or "Don't know" to even one of these questions, your critical processes could be vulnerable to a business-crippling disruption.

**Can you identify your critical business activities that satisfy your customers' expectations and support your overall business operation?**

Yes     No     Don't know

**Can you identify the critical business information needed for these activities to succeed?**

Yes     No     Don't know

**Do you have information on the frequency, impact and causes of downtime?**

Yes     No     Don't know

**Does this information allow you to identify and rank your most vulnerable business activities?**

Yes     No     Don't know

**Are your legacy systems and IT resources adequately protected against hacker intrusions and viruses?**

Yes     No     Don't know

**Have you developed a checklist, by functional area, of what your company will need to continue business effectively in the case of a disruption or emergency?**

Yes     No     Don't know

**Have you and your IT colleagues successfully placed business continuity on the board agenda?**

Yes     No     Don't know

**Have you worked with your IT colleagues to develop an approved business continuity plan that accounts for all aspects of business continuity and recovery?**

Yes     No     Don't know

**Is your business continuity plan regularly tested?**

Yes     No     Don't know

**Do you have a change control process in place to keep your continuity plan current with process, organizational and technology changes?**

Yes     No     Don't know

**Are you confident that if a disruption or disaster struck this minute, your organization could recover quickly and smoothly enough to prevent damage to your business?**

Yes     No     Don't know



## Critical success factors

### What to look for in a business continuity service provider

Today, many vendors offer business continuity and disaster recovery services and solutions. Services can include consulting, planning, hardware, software and alternative facilities equipped for IT or call center operations.

The service provider you choose must deliver support that addresses your company's critical business processes. Listed are some of the key success factors to remember when evaluating a service provider's ability to deliver true business continuity solutions:

- The ability to understand the integration of IT with business strategy, and define the risks and impacts of a disruption to critical IT infrastructures
- An understanding of e-business dependencies and business-critical requirements
- A focus on business continuity, separate from traditional disaster recovery services
- An understanding of supply chain dynamics
- Skills and resources to manage complex continuity programs in a rapidly changing, networked IT environment
- The ability to draw upon resources outside of core continuity and recovery skills
- A formal intellectual capital management system that allows best practices and up-to-the-minute procedures to be shared worldwide
- Extensive experience across a wide range of industries, geographic regions and disaster scenarios
- Sufficient resources to accommodate multiple recovery clients in the event of a widespread disaster
- Support for multivendor, multiplatform IT environments
- Access to world-class researchers, facilities and technology developers
- A significant investment in state-of-the-art facilities and tools, and the financial wherewithal to continue investing
- Integrated solutions to assure availability of non-data center resources, including networks, end-user workspace and call centers
- A proven track record in recovery and technical support
- A seamless interface to additional services and support
- Access to the latest technology, constantly refreshed to reflect the needs of the market.



## **About IBM Global Services**

As one of the world's largest business and information technology services providers, IBM Global Services has the knowledge, skills, experience and unsurpassed breadth of capabilities to manage and deliver business continuity and recovery services.

We offer a continuum of solutions that range from consulting, planning and testing for business continuity implementation to full management of business continuity for your critical ERP, e-business and strategic processes. We also provide recovery services and facilities for large, midrange, distributed and multiplatform computing environments, as well as network and call center recovery.

The source of our strength is our people—more than 130,000 professionals in more than 164 countries. They come from diverse backgrounds—business continuity experts, e-business consultants, high-availability professionals, technology specialists in multivendor environments, professionals in IT operational management and IT support specialists.



### Summary

Business continuity is so vital to business success now that it can no longer remain a concern of the IT department alone. The time, money and customer confidence that can be lost due to downtime or business interruption can seriously damage a company of any size—and the reputation of its key executives—both short and long term.

The risks are even greater for e-businesses and companies that operate in the 24-hour, 7-day-a-week global environment. To assure survival, companies must adopt proven strategies to protect both business processes and vital information and implement corporate-wide programs for continuity and recovery management.

To learn more about how your company can benefit from putting the people of IBM Global Services on *your* team, visit [www.ibm.com/services/continuity](http://www.ibm.com/services/continuity), contact your sales representative, or e-mail us at [ibmbcrs@us.ibm.com](mailto:ibmbcrs@us.ibm.com).



## References

- <sup>1</sup>Dalton, Gregory. "E-Business Emergency — The High-Stakes Battle For Online Customers and Market Share Has Turned Crisis Management Into A Top Priority." *InformationWeek*, September 6, 1999.
- <sup>2</sup>Strategic Research Corporation, Peterson, Michael and Newton, Kris, "1998 DATABASE OPERATING PRACTICES High Availability and Data Protection, Executive Summary." [http://www.sresearch.com/oper\\_prac98.htm](http://www.sresearch.com/oper_prac98.htm).
- <sup>3</sup>Patrowic, Lucie Juneau, "A River Runs Through It." *CIO Magazine*, April 1, 1998.
- <sup>4</sup>DiDio, Laura, "Computer Crime Costs on the Rise." *Computerworld*, April 20, 1998.

© International Business Machines Corporation 1999

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

Produced in the United States of America  
10-99

All Rights Reserved

IBM and the e-business logo are trademarks or registered trademarks of International Business Machines Corporation.

All other registered trademarks, trademarks and service marks are the property of their respective owners.

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