July 2006

Trend Advisory

information > intelligence > insight

Disaster readiness and recovery planning

Hurricanes, power outages and dozens of other threats can shut down your business in a matter of minutes. Is your data center prepared to weather the next catastrophe?

published in association with ZIFF DAVIS

Hoping for the best, but preparing for the worst

There's no way to predict when disaster may strike, but smart strategizing now can save time and money — if not your entire business — when the time comes.

EMERGING TRENDS

Cyber-threats, natural disasters, regulatory compliance driving business continuity plans

Hurricanes, denial of service attacks and even electrical failures may devastate a business, but a resilient operation is ready with off-site data storage, backup power and a crisis response plan.

SOLUTION INSIGHTS

The company you save may be your own

A comprehensive disaster plan starts with a thorough analysis of your I.T. needs and a cost analysis of each preparedness measure.

I.T. BEST PRACTICES

I.T. and management collaboration crucial for contingency planning

Experts agree that I.T. administrators, business users and executives must work together to set policy for company-wide crisis response and operational recovery.

UPCOMING PRODUCTS

Prepare now and avoid disaster

Disasters are far less devastating when you have the right equipment, including uninterruptible power supply systems, off-site backup media and top-notch network hardware.

EMERGING TRENDS

Cyber-threats, natural disasters, regulatory compliance driving business continuity plans

What do you do when a disaster shuts down or destroys your company's technology infrastructure?

Depending on which report you read, analysts call the answer to this question disaster preparedness, disaster recovery, business continuity, business resiliency and even information stewardship.

Whatever term you use, your company must answer to customers, employees, and industry and governmental regulations, regardless of how mundane or outlandish the problem. It doesn't matter whether a construction crew severs your building's power lines or a hurricane levels the city; you have to be prepared.

Disasters come in all shapes and sizes. A virus attack can bring down your network as easily as a power outage can, and an electrical fire or flood can be as devastating as high-profile events like Hurricane Katrina. Worse, there's no way to predict where and how the next catastrophe will strike.

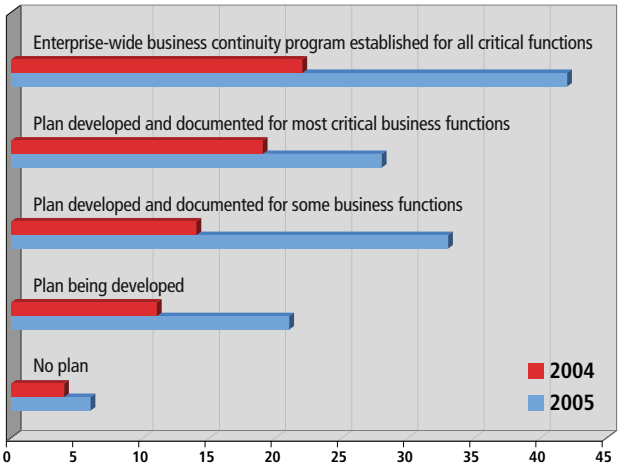
In a June 2005 survey conducted by Risk Solutions, LLC, 62 percent of respondents listed data security (virus, denial of service, unauthorized access) as an "extreme threat" to their business continuity, with power outages, telecom failure and data-center failure close behind.

Respondents also listed fire, natural disasters, flooding and violence/terrorism as important issues to consider when creating a business continuity plan.

On the most basic level, the damage and downtime resulting from a disaster can have dramatic effects on a company's bottom line. Every hour of downtime brings mounting costs, and the repercussions in terms of corporate reputation and customer retention may still be felt over the long term.

In a survey conducted by Contingency Planning & Management (CPM Group) and Deloitte & Touche, nearly half of respondents indicated that their businesses could not tolerate more than eight hours of downtime and must have critical activities restored within that time frame. More than 12 percent of respondents indicated zero-tolerance, demonstrating that resilience — the ability to bounce back quickly — is a must when creating a business continuity plan.

Do you have a business continuity plan?



Enterprise business continuity program development has taken hold, with implementation being reported by at least 70% of respondent companies in 2005, up from 41% in 2004. (Source: CPM Group and Deloitte & Touche LLP 2005 Business Continuity Survey)

"We went around the organization identifying what the business thinks they have in terms of a business continuity management requirement and then compared that to what they actually had. There was a disparity."

– Bill Teuber, CFO and executive vice president, EMC Corp.

EMERGING TRENDS (CONTINUED)

Regulatory compliance is another major factor when considering how careful your company must be when handling customer data. The New York Stock Exchange, for example, requires its members to develop business continuity plans and update them annually. A regulatory standard for business continuity management is under development in the United Kingdom.

Regulations such as Sarbanes-Oxley, HIPAA, the California Database Breach Notification Act, the Gramm-Leach-Bliley Act and the European Data Protection Directive will also drive additional focus on data protection and disaster preparedness.

An April 2006 article in *Business Finance* cites a report from risk consultants Nicholas Benvenuto and Brian Zawada, who note: "[A] growing number of executives have been influenced by their external auditors, who have knowledge of business continuity and the potential risks. As a result, they are concluding they must have business continuity processes, or at least be able to show why they do not have the processes, related to their financial reporting function (and perhaps extend this assessment to other critical business functions and IT assets at a later date)."

The story also quotes Peter Maloney, CFO of digital licensing firm Snocap, as saying: "Companies may have had informal procedures and processes for disaster recovery, but Sarbanes-Oxley has forced a formalization of those procedures and processes."

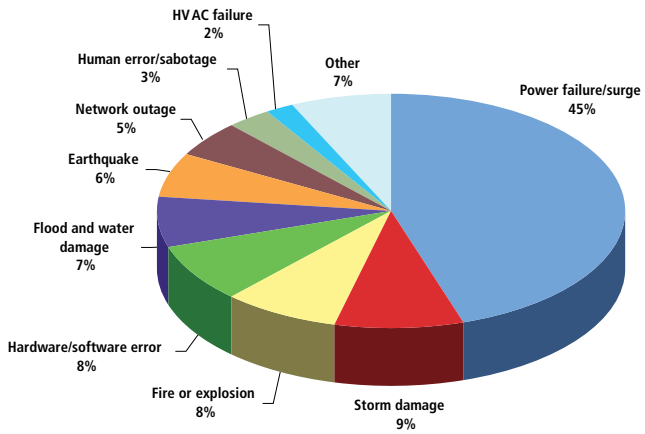
In the Risk Solutions survey, 78 percent of respondents cited regulatory requirements as driving their business continuity plans.

For compliance purposes, companies have to ensure that data is protected and archived according to established regulations.

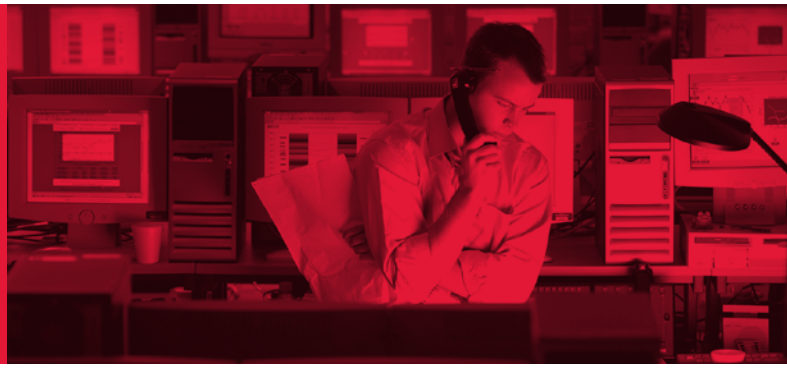
Disaster preparedness dovetails nicely with this trend, giving companies an opportunity to add off-site storage to their data management initiatives and redundant power sources for their data centers.

By ensuring that critical data, system configurations and even up-to-date inventory lists are stored securely away from the main office, businesses can recover quickly from an event that would prove devastating to an unprepared company. If a flood damages a data center in one location or a power outage takes out the entire Northeast (as we saw in August 2003), a business continuity plan will mean the difference between smooth resumption of activities and a chaotic scramble to recover.

Major causes of power problems for PCs



Your company's server and PC hardware resources are susceptible to power fluctuations from many different sources. To protect critical corporate and customer data, a continuity plan should include surge protection and uninterruptible power supply systems. (Source: CPM Group, 2004)



SOLUTION INSIGHTS

The company you save may be your own

A solid disaster-preparedness plan starts with a thorough analysis of what may go wrong, what has to be saved (at nearly all costs) and how to implement a strategy that encompasses people, processes and equipment.

In a December 2005 report, Nemertes Research analyst Melanie Turek finds that 87 percent of I.T. executives say information stewardship — managing and setting policies for every byte of data in the enterprise — is vital to their organizations, but only 40 percent rank it as important when allocating funds and resources.

It's important to note that establishing a disaster-recovery plan does not necessarily require heavy spending. "Don't think about disaster planning as a task separate from the general imperative to manage records properly," say Gartner analysts Kenneth Chin, Toby Bell and Debra Logan in a 2005 report titled *Advanced Planning Can Save Your Records From Disasters*. "You need to take only a few extra steps in your records management program to reduce the risks from disasters and to recover records if disaster does strike."

Storage and security provider Iron Mountain identified several steps in planning for disaster and subsequent recovery.

1. Determine how the event will impact four key areas:
    - People: How will you notify, evacuate, transport and care for employees?
    - Property: What equipment will you need and how will you source it?
    - Systems: What portions of your computing and telecommunications infrastructure must be duplicated immediately? How much downtime can your operation tolerate?
    - Data: What data is critical to run your business, and how will you recover critical data that is lost?
2. Determine which data, applications and systems must be restored and in what sequence. Prioritize systems as critical, vital, sensitive or noncritical, and talk to users at all levels to make sure you're not overlooking any crucial systems.
3. Analyze the hardware and software configurations that support critical business functions and isolate possible points of failure.
4. Quantify hourly costs based on interruptions of these systems.

Iron Mountain lists several different types of outages, including branch offices going offline, local and regional power disruptions, and application failures that may force a data center offline.

A business continuity plan must include strategies for secure off-site storage of critical company data. This includes customer databases, company e-mail, financial records, and order and inventory databases. Executives and I.T. staffers have to work together here to set policies for the whole organization.

Make sure you have the appropriate safeguards (firewalls and antivirus scanning) to verify the data's quality, and then set up a storage plan that protects critical information securely. Information lifecycle management (ILM) software, together with backup management and data recovery software, put a management interface over the system and enable you to fine-tune the security to your company's needs.

In addition to tiered and off-site storage, electrical power should figure prominently in your plan. A sudden power outage can wipe out worker desktops and server caches, causing very expensive losses. Uninterruptable power supply (UPS) systems ensure that equipment can be properly shut down, databases opened and files saved in time so no data is lost. Combining this type of protection with secure off-site servers and storage is essential for proper backup and recovery to all your critical data.

I.T. BEST PRACTICES

I.T. and management collaboration crucial for contingency planning

When planning and executing a business continuity program, I.T. managers need executive buy-in. The best way to do that is to present well-researched numbers, indicating the costs that will be incurred in case of a disastrous event. Eric Krell, writing in *Business Finance* magazine (April 2006), reports that finance departments are increasingly recognizing the danger in leaving business continuity to chance and can serve as a valuable ally for I.T. when making the case for disaster preparedness.

Phil Bloodworth, a Dallas-based advisory partner with PricewaterhouseCoopers, suggests that plans be put in place for individual processes. If a particular set of resources supports certain high-priority operations, the staffers in charge of that section should outline a protection scheme and an alternative track if the resources are compromised.

On a higher level, Bloodworth adds, a business continuity plan describes how the company's people, processes and technology will function during an unexpected event. This plan should also detail the measures your company has in place to limit the negative impact of a disaster.

This plan should not be monolithic, he warns, but a "living, breathing" process that is updated regularly to reflect organizational changes.

Businesses must also be ready in case an emergency threatens employee safety. These programs lay out the roles and responsibilities of managers and employees during an event. An organizational chart is helpful in outlining responsibilities, reporting lines and communication rules. "How will the company inform its employees about the emergency and about what they should do? How will it communicate with suppliers, customers, shareholders, the communities in which it operates emergency response officials, regulators and the media?" Bloodworth says, are all questions to be addressed in a crisis management plan.

The U.S. Small Business Administration offers the following tips to recover systems and restore business processes quickly:

- Keep a backup copy of your computer operating system, boot files and critical software offsite
- Save an up-to-date copy of network log-on accounts offsite
- Keep system configuration lists offsite, so you can order replacement equipment quickly
- Compile a list of phone numbers and develop a telephone tree to contact employees in an emergency

Gartner analysts Kenneth Chin, Toby Bell and Debra Logan urge companies to approach disaster recovery from a records management perspective. They suggest:

- Create an inventory of your records so that you know the volume and where they're located
- Evaluate the importance of each record and create a retention schedule for each type of record
- Assign staff to verify locations of important records
- Create electronic copies of key paper records
- Store imaged records and other backups offsite; the backup location should be far enough away that it won't suffer if a major disaster strikes the city in which you have your frontline offices, yet not so far away that you can't recall the records conveniently
- Devise secure procedures for recovering records from the backup locations and testing them periodically

Most companies have their recovery sites less than 50 miles from their production sites, the analysts write, and a disaster like Katrina may disable both sites. Companies that are located in high-risk areas should keep a third copy of their most critical unique records at a site outside the region.

"Many companies know they have an issue, but there are so many business units, processes, applications, networks and servers that paralysis can set in."

– Steve Higgins, EMC director of continuity and security solutions

UPCOMING PRODUCTS

Prepare now and avoid disaster

Disasters can come in many forms, and the best way to ensure resilience and continuity is by having UPS systems to protect data in case of an outage and tiered storage to protect data in case of physical damage.

Rack-mount or stand-alone UPS systems, such as the APC Symmetra RM, kick in and provide up to 12 minutes of additional power to network devices, so users and I.T. staff can save all work and bring down the servers correctly. The alternative is blink-of-an-eye shutdown for the entire data center, leaving chaos and confusion in its wake.

High-speed, low-cost storage is the next crucial element in a backup and recovery plan. The EMC CLARiiON UltraScale CX3-20 is the entry point to the UltraScale series, and it offers exceptional scalability and throughput for up to 120 connected drives — a potential 60TB of storage capacity.

Backup software manages the tiered system with automatic scheduling and intelligent routing of information to disk- or tape-based storage media. The best-in-class solutions let I.T. managers virtually "set and forget" backup activities, requiring intervention only once a week (or less frequently) when it's time to revolve the media. Symantec's Backup Exec 10d *for Windows Servers* offers all these features and includes a Web-based management interface that lets you recover files from any browser.

Speed and intelligent traffic management options are key components of any network's resilience. Although Fast Ethernet delivers respectable 100Mb/sec speeds over Ethernet, the latest network hardware supports Gigabit Ethernet — which is 10 times faster — and thus optimal for increasing data loads, voice over IP applications and video traffic. Cisco Catalyst switches bring high speed and intelligent, dynamic packet routing to your network, enabling your business to take full advantage of cutting-edge computing technologies.

APC Legendary Reliability®

APC Symmetra RM

Caches can be flushed and critical work may disappear in the crucial minutes after a power outage. With an APC rack-mountable power supply, you can buy enough time to bring the network down smoothly.

EMC² where information lives

EMC® CLARiiON® CX3 UltraScale™ series

Data volumes, regulations and disaster threats are all increasing. EMC answers the call with high-speed, highly scalable storage solutions for midsize companies in its CLARiiON series of networked devices.

symantec.

Symantec™ Backup Exec™ 10d *for Windows® Servers*

Whether you're using tapes or hard drives, Symantec's Backup Exec 10d *for Windows Servers* is the package of choice for your critical server data, providing continuous protection, intuitive management and even Web-based file recovery.

Cisco Systems | Authorized Reseller

Cisco® Catalyst® 3750-24TS Switch

The best way to help a business run smoothly and recover quickly is to have the best network hardware delivering resilient service from the start. Cisco Catalyst switches offer Gigabit Ethernet mechanisms for marking, classification and scheduling.

Technical Specifications

CDW is your disaster-preparation partner, with the hardware, software and expertise you need to add security and resilience to your data center. Whether your plan calls for UPS systems, high-speed/low-cost storage devices, software to ease I.T. headaches and streamline backup processes, or a combination of business continuity products, CDW has the widest selection and the most helpful technicians.

APC
Legendary Reliability®

APC® Symmetra® RM

Redundant power protection with scalable power and runtime

Whether your storage is direct attached, network attached or anywhere between, APC has a solution that can help you improve your application's availability. Add APC power protection to your storage devices to ensure the cache is maintained during a momentary power outage.

- 2000VA, 1400-watt, 14 outlets
- Ideal for branch office locations or mission-critical networking equipment
- Features hot-swappable, user replaceable battery

CDW 237487

Cisco Systems
Authorized Reseller

Cisco® Catalyst® 3750-24TS Switch

24-port 10/100/1000BASE-T managed, stackable (up to 9 units) and rack-mountable switch with SMI installed

The Cisco Catalyst 3750 Series Switch is an innovative product for medium to large-size organizations and branch offices. Featuring Cisco StackWise technology, this switch improves LAN operating efficiency by combining ease of use and the highest resiliency available for stackable switches.

- Optimized for high-density Gigabit Ethernet deployments
- Scalable up to 252 gigabit ports
- Supports IPv6 routing for maximum performance

CDW 497268

symantec.

Symantec™ Backup Exec™ 10d *for Windows® Servers*

Designed for disk, delivering more reliable, faster and more efficient data protection

Symantec™ Backup Exec™ 10d *for Windows® Servers* is an industry-leading Windows® data protection solution designed for disk, providing comprehensive, cost-effective and certified backup and recovery — now including true continuous data protection with the industry's first Web-based file retrieval. Centralized administration provides scalable management of distributed backup and remote servers.

- Self-service file recovery without requiring I.T. intervention
- Reduces operational cost in Microsoft® Windows environments
- Increases Windows application availability
- Reduces administrative cost
- Provides granular protection for a wide variety of applications

CDW 923330

EMC²
where information lives

EMC® CLARiiON® CX3 UltraScale™ series

The powerful CLARiiON® CX3 UltraScale™ series of networked storage systems delivers maximum business benefits with new levels of performance, scalability, flexibility and ease of use.

The CX3-20 is the entry point to the UltraScale series. With four 4Gb/sec front-end and two 4Gb/sec back-end connections, it scales up to 120 drives, 60TB of capacity and 128 high-availability (dual-connected) hosts.

CDW 986822

Contact your CDW account manager, visit CDW.com or call 800.800.4239 for more information on disaster-preparedness solutions.

CDW®

The Right Technology. Right Away.™
CDW.com • 800.800.4239

published in association with ZIFF DAVIS