Today’s IT- and online-intensive business environment requires “all-the-time” uptime. Certain applications, data and any associated IT infrastructure — for example, sales and support — need to be available 24x7, not just 9-to-5 Monday through Friday.

Of course, some companies can tolerate minutes, hours and even days of IT outages. For others, even a few-minute slowdown or unavailability can mean millions of dollars in missed revenue, lost customers and negative impact on a company’s stock price.

In a survey published by Enterprise Strategy Group, Data Protection Market Trends, in February 2008, “For the most critical applications, a majority of organizations (63 percent) cannot tolerate more than four hours of downtime without significant adverse impact to their business.” Experts say it probably is even less today.

The same survey, which talked with organizations in the 100-to-1,000 employee range, stated that 40 percent of respondents could tolerate less than four hours of downtime. While 18 percent stated that they could tolerate less than one hour of downtime, 5 percent said no downtime was tolerable.

Downtime often equals lost revenue. And in today’s world of economic malaise, such events can be even more precarious. Even though budget restrictions are the order of the day, Business Continuity (BC) and Disaster Recovery (DR) planning remains a high priority.

Staying in business takes a solid core strategy. A combination of effective data backup, high availability, resilient networking and archiving strategies can prove effective in beating downtime, especially during times of economic distress.

Business Disruption
Today’s IT infrastructures face varying risks of interruption due to a myriad of different reasons. Events — large or small — can interfere with IT availability.

Heat waves can lead to rolling power brown-outs or outages. Floods or blizzards can close roads and make buildings inaccessible. Meanwhile, hurricanes and tornadoes may force general area-wide evacuations, even destroy office buildings and data centers.

A pandemic can keep people from coming to the office. A backhoe can sever a fiber-optic link. A delivery truck can knock down a utility pole. Even something as small, local and simple as an accidentally-unplugged power or network cable, a hard drive failure or a missed software patch can result in a major IT-interfering event.

Given the growing reliance on IT, combined with the potential for network downtime, companies of all types and sizes are putting more emphasis on keeping mission-critical services running. The strategy includes finding the best ways to avoid or minimize the impact of a disruptive event.

Upfront Planning
Business continuity is about keeping the business running. It’s a plan for backing up the data directory along with the accompanying application, thereby allowing the business to get back up and running with minimal delay.

Disaster recovery is the ability to make some or all stored data available following a disaster. It means something went down and you need to get it up and running. It also means that you need to get your data back to some point in time.

Risk mitigation is often defined as the strategies used to reduce either the probability or consequences of a direct threat. According to Greg Schulz, founder and senior analyst of the StorageIO Group, “It includes taking the steps to avoid or minimize applicable threat risks.”
When it comes to risk mitigation, not all data or applications are equal. "IT first needs to take inventory of the applications and business processes that are part of the environment," says Rick Walsworth, director of product marketing, EMC Cross Platform Replication, EMC Corp.

“They then need to define which of those are mission critical," he adds. Following that applications will be categorized as "business-critical" or "less-than-critical."

Organizations need to look at how much data you can afford to lose in the event of a failure. “That's your Recovery Point Objective or RPO," Walsworth explains. RPO is typically measured with a clock, not a calendar. Some firms look at an RPO of seconds or even zero-tolerance.

Recovery Time Objective (RTO) is how fast you can restart applications after the data has been recovered. “When a company looks at their acceptable risk for data loss and for downtime, you have to include the RPO and RTO," Walsworth adds. “Then you need to design for that.”

**Tools of the Trade**

When it comes to BC and DR planning, certain protocols must be in place. Every good plan employs certain technologies and methodologies to limit the disruptiveness of an outage.

Firms need to document not only the business functions, but also all the elements of how to recover the technology components. That is to say, the “how to do it” is just as important as the “what to do.”

“There are studies that show that having the right processes and methodologies in place will probably prevent a good 50-to-60 percent of the issues that crop up,” says Ravi Pendekanti, VP of worldwide sales and marketing at Overland Storage.

**Backup** — Replicating your data is essential in today's business climate. An organization's most valuable resource is data, and one of its most important tasks is to protect it. Replication methods come in numerous forms, from tape to Disk-to-Disk (D2D) to Disk-to-Disk-to-Tape (D2D2T), etc.

“Backup is a basic,” says Lauren Whitehouse, an analyst at the tech analyst firm Enterprise Strategy Group. “Most companies make a copy of production systems’ data and keep one copy locally for operational recovery and one copy remotely for disaster recovery.”

**Document Management and Archiving** — important components of compliance, document management and archiving are typically used for long-term data retention and records management. By ensuring that a firm's documents and records are properly maintained and accessible, document management solutions can help play a major role in a business continuity plan.

Document management represents a systematic approach to digitizing, storing, managing and retrieving documents. When properly implemented, it can allow your crisis team to have access to critical documents during times of disaster or disruption.

A systematic approach to storing, managing and searching for files, e-mails, Instant Messages (IMs) and other application data, archiving automates the process of moving data from primary to secondary storage. It also serves to automate the retention, deletion and legal review process for files and e-mails.

“When you are in a disaster, it is chaos. And if it is documented who needs to be contacted, how to contact them, and when to do so, then you are going to be headed in the right direction,” notes Marc Johnson, managing director of Data Center Transformation with Symantec's Global Services.

**Offsite Storage** — Once your data has been saved and replicated, moving it to an offsite storage location is the next logical step. Offsite storage is fail-safe for a local outage or disaster, allowing your data to be easily recovered.

While it may make sense to own a secondary site, it may be more practical to use a secondary storage site that is hosted by a vendor. Using this hosted site leverages shared resources. For some businesses, the use of a collocation facility may be the best bet for a secondary data center.

**High Availability** — HA refers to a strategy which allows for nearly 100 percent accessibility of systems. It serves to create business resiliency, helping to prevent a single point of failure.
Through the use of replication technology, clustered servers, disk arrays, storage area networks and offsite locations, HA creates redundant systems which can be switched on instantly in the event of a primary failure.

“Our portfolio of products does proactive management — if you do have those plans and strategies in place — to use high availability across geographic clusters,” says Johnson. “In addition, we can use a local cluster to eliminate the need to failover from one data center to another.”

Network Resilience — Organizations today operate within a global environment. Transactions can take place 24x7 — anywhere in the world. Consequently, networks have to have multiple layers of diversity built-in to mitigate risk.

Network resilience is often referred to as the methodology used to assure that a network is tolerant to failure. According to the experts, configuring resilience into the network includes analyzing how much you need and where you need it most.

Virtualization — The flavors of virtualization technology, especially server virtualization, can play a big role in DR strategies. Server virtualization removes the one-to-one requirements of physical environments, lowering costs and simplifying DR environments. And along with replication, it enables low-cost mirroring.

“IBM offers a significant amount of products in this area,” says John Sing, an IBM Systems Group senior consultant for Business Continuity Strategy and Planning. “Our advantage is that we offer virtualization, backup, document management, HA, archiving, etc. in a holistic and integrated way across all our product lines, including servers, storage, software, automation and services.”

Cost Assessment
In looking at the costs associated with an overall business continuity strategy, it is important to first understand the costs of not having one in place. The risks attached to not having a BC or DR plan are neither small nor cheap.

It is almost universally believed that Total Cost of Ownership (TCO) of a good BC strategy and DR plan is less expensive than the fallout of a disruptive event when there are no such plans in place. And when compared to going out of business, having a plan in place is a far more desirable option.

Cost of Downtime — While the cost of downtime varies drastically by industry and organization, it is clear that downtime equals loss. Per hour, these figures can run anywhere from the millions, for brokerage operations, to tens of thousands, for things like banking ATMs.

Also, there are more things than just dollars and cents which may be lost as a result of downtime. Brand reliability and customer trust is a significant loss.

This ties in closely to the notion of market share. A major disruptive event could lead to your piece of the pie being taken by a competitor. With a loss of customer trust, it is possible that you may never get some of them back.

Amount of Protection — “Similar to applying insurance against assets, you can compare the value of the company’s assets — what would constitute the expected loss in a disaster — against the costs of protecting them,” says Enterprise Strategy Group’s Whitehouse.

An enterprise’s cost of protecting those assets is similar to the premiums paid for insurance. The concept is the same. Knowing the acceptable amount of coverage and the amount one is comfortable paying for is paramount.

“Examine the company’s assets and determine the value,” she notes. “The value could be based on replacement cost, the cost of lost productivity or the lost revenue without the asset, fines or legal ramifications. Or even if the asset is lost, the value of the asset to the company,” she adds.

How Much to Spend? — The first thing that must be spent is time. Firms must do their due diligence in determining what is right for them. The old carpentry adage of “measure twice and cut once” holds true for BC/DR planning as well.
That said, there are once again no hard figures which can be provided. However, there are some generalities that can be made.

“In fast-recovery scenarios, it’s not unusual for ongoing network bandwidth costs to be 50-to-70 percent of the overall TCO of the BC solution over the course of three to four years,” says IBM’s Sing. “Networking costs dwarf everything else.

“Therefore to be cost effective, businesses need to either limit the amount of data/applications that can be recovered in a short time frame, or they accept the longer time frames for recovery because that’s what’s affordable,” he says. “They have to accept the risk as the tradeoff.”

And finally, while a company’s BC plan spending seems to be a function of the amount of protection that it wants, weighing in factors like RTO, RPO, hardware, software, bandwidths and even real estate is appropriate regarding some general rules that should be considered.

**Ensuring Business Continuity: The ABCs**

- **Have a plan in place** — Though it sounds simple, simply making sure that a proper Business Continuity (BC) plan is available is half the battle. Here the focus should be on setting the right expectations and on understanding what resources are most important.

- **Take a program approach** — Think of BC as a program and not merely as a project. BC is dynamic. As your business changes, so too should your plan. While there may be a beginning, there is not a true end to BC.

- **Testing, testing, testing** — It is essential to test your plan once it is in place; and not only initially, but on an ongoing basis. Furthermore, firms should make sure they are doing the right kind of testing. Completing 100 percent of your tests correctly just isn’t realistic, and organizations should plan on failures occurring.

- **Monitor your work** — Regular reviews of network security should be scheduled. Monitoring your data will help guard against unauthorized access, and will help prevent the modification, deletion and theft of data.

**CDW OFFERS STORAGE, POWER AND NETWORKING SPECIALISTS TO ASSIST WITH DISASTER RECOVERY NEEDS. CALL 800.800.4CDW TO TALK TO A SPECIALIST TODAY.**