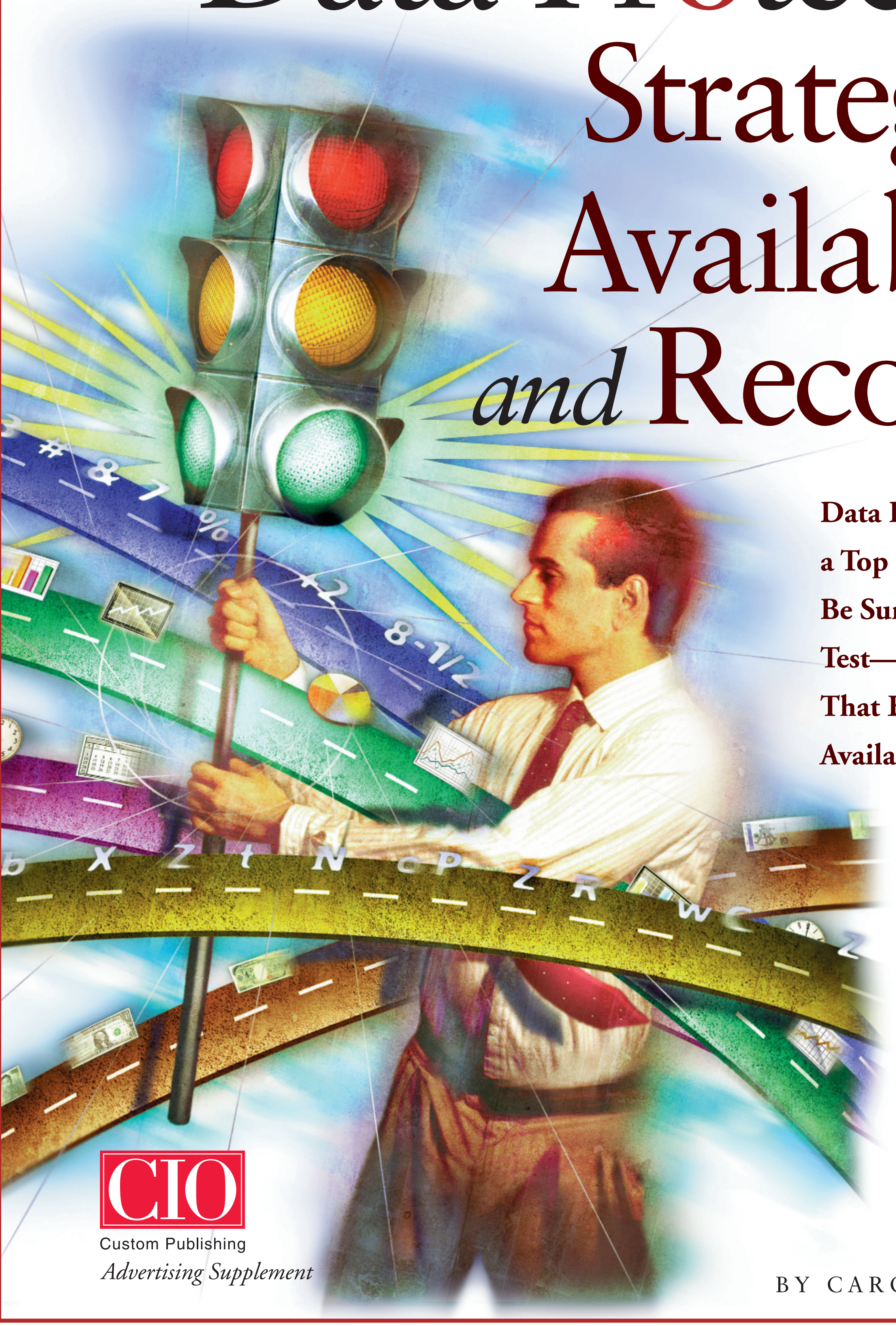
How to Build a Data Protection Strategy *for* Availability *and* Recovery

Data Protection Isn't Just a Top Priority, It's a Must. Be Sure to Develop—and Test—a Storage Strategy That Emphasizes Data Availability and Recovery.



CIO
Custom Publishing
Advertising Supplement

BY CAROL HILDEBRAND

How to Build *a* Data Protection Strategy *for* Availability *and* Recovery

Could you do business without faxes? It'd be painful, but there's always FedEx. Your phones? That's a tough one, but if you had to, you could. How about computers? That's a whole different story. Computers hold the lifeblood of any new economy corporation: databases of customer buying habits, online inventory tracking systems, collaborative email systems where professionals share ideas via audio, video and electronic documents. Even more compelling, savvy executives can mine these treasure troves of stored information to glean a competitive advantage and boost profits.

But only if they have the data. Consider what would happen if Amazon or Land's End could not use its web site to sell goods and service customers. Or if Wal-Mart couldn't use its distribution system to make sure that merchandisers got the right products to the right place at the right time. Or if Pfizer couldn't use its knowledge management system to speed up its patent application process. The answer boils down to more than a short-term dip in revenue. "Catastrophic loss of data can—and does—close down businesses," says Greg Meland, the president and CEO of Datalink, an information storage architect based in Minneapolis, Minn. Indeed, some corporations faced with data losses from September 11 were unable to continue as going concerns.

Data protection must be a top business priority, and that means companies must develop storage strategies that emphasize data availability and recovery. After all, storage is the vessel that holds this treasure trove of information—information that

BY CAROL HILDEBRAND

must be at the fingertips of employees when and where they need it. Safeguarding and accessing that information has become increasingly vital, and a comprehensive data protection plan lies at the heart of that ability. “In today’s market, time is money, and inaccessible data or systems are not acceptable for information-savvy executives and our business customers,” says Michael O’Brien, Director of North American I.T. for Datex-Ohmeda, a division of Helsinki-based Instrumentarium Corp.

In order to satisfy the demands of these information-savvy executives, “systems must have very little downtime—in other words, high availability,” says Meland. “But if disaster should strike, executives also need a reliable strategy to recover the data and get systems back up as fast as possible. Data protection spans both availability and recovery, and companies should pay attention to both sides of the equation.”

With the very future of a business riding on this decision, you’d think that most companies would have long ago created detailed data protection plans. After all, that’s the necessary first step to ensuring that corporate data remains safe and recoverable in the event of natural disasters, terrorism and other massive ruptures in the fabric of day-to-day business.

But you’d be wrong. “It’s extremely rare to find an organization that is well protected,” says Tom Sylvester, Datalink’s senior director of technical services. “When you look at what plans companies have in place, very few are comprehensive. And I don’t think they know.”

The Disaster Readiness Consortium reports that of the thousands of businesses who have taken the Disaster Readiness Scorecard of best practices:

- 75% are in the **Danger Zone**
- 21% **Need Improvement**
- 4% meet **Best Practices**

According to Pat Martin, the president and CEO of StorageTek, a storage solutions provider based in Louisville, Colo., “While many organizations claim to have a disaster recovery [DR] strategy, the majority of the strategies are unexecutable due to outdated plans, lack of internal expertise, and inadequate testing processes. Organizations, especially those who depend heavily upon technology to operate, need to understand the costs of unplanned outages and weigh those costs against an acceptable risk management profile.”

And more companies than ever before are interested in data availability and recovery, particularly in the wake of the tragic events of September 11. “It really has made people think, ‘This could happen to me,’” says Diane McAdam, an analyst at Illuminata, a research firm based in Nashua, N.H.

Conseco Finance

Headquartered in St. Paul, Minn., Conseco Finance has been providing loans for manufactured housing, home equity and home improvement since 1979. Conseco Finance is a part of Conseco, an insurance and financial services firm with approximately $94.6 billion of managed assets.

Conseco Finance maintains four separate data centers in St. Paul, Tempe, Ariz., Duluth, Ga. and Rapid City, S.D. Chief Architect Rod Lucero estimates that the company has 43+ terabytes of raw data. Like most companies in the financial sector, Conseco Finance stores a lot of data, is heavily dependent on it, and is very proactive when it comes to data protection. Conseco also runs a number of SANs.

Backup and Recovery

Conseco Finance maintains multiple data centers with identical technology, says Rod Lucero, the company's chief architect. "If I do a backup in St. Paul, I can take the tape to Tempe and that center has the same infrastructure that's capable of reading it." It also has remote asynchronous volume replication over existing TCP/IP network infrastructure.

Conseco runs frequent tests of its data protection plan to ensure that it remains in compliance. One result was that it recently discovered that some systems were outside the prescribed timeframe for backups as defined in the company's internal service level agreements. In fact, one backup took more than 24 hours. The company worked with Datalink to develop and implement a local and remote data protection strategy and architecture.

Results

Backup times were reduced by 50 to 66 percent the normal times. By using the SANs, Conseco has improved availability and tape drive utilization.

It's not a simple task, however. In order to build an acceptable risk management profile, smart executives must first identify a host of challenges to be overcome before they can build a secure data availability and recovery strategy.

Identify the Challenges

Companies must deal with the increasing technical complexity of storage.

Storage used to be a relatively simple concept. The IS department would hang a storage device off of each server or mainframe unit, and back them up to tape. But as corporations seek to interconnect various pools of data in their efforts to wring a full measure of worth from enterprise systems such as ERP and CRM projects, storage has grown steadily more complex. Instead of direct-attached storage, storage units have moved onto the network, or companies have built storage area networks (SANs) to further integrate storage into the corporate infrastructure. As a result, the array of software and hardware a large company uses for storage has multiplied faster than bunnies in the night. For example, a traditional storage setup generally involves only one or two vendors. But a typical SAN is much more complex, utilizing more storage software and networking technology on top of the hardware. As a result, it uses products from five to seven vendors. "Most people think disaster recovery is simple because they think, 'I replicate and I'm done,'" says Illuminata's McAdam. "It's just not that easy anymore."

The additional technology layers mean that IS departments must work harder to manage the SANs, allocate storage capacity and integrate the various products. In fact, ever larger portions of IS storage budgets are being spent on software rather than hardware. The result: All that technology means that CIOs have many more factors to consider when they create and maintain data protection plans.

Storage capacity needs continue to skyrocket.

Adam Couture, an analyst at Gartner, reports that the demand for storage capacity will balloon from 283,000 terabytes in 2000 to more than 5 million terabytes by the middle of the decade. There's another wrinkle, too: Even though analysts say that prices for technology such as big disk drives are declining at a rate of 35 to 40 percent a year, the continued corporate appetite for storage means that it will remain a significant line item on the corporate IT budget—as much as 50 percent, according to some analysts. What's the bottom line on all this? Executives have made a significant investment in data storage. As they continue to pour money into this sector, the ever-increasing cache of data becomes more difficult to protect.

Uptime demands are more stringent. For many businesses, it used to be just annoying when email went down; now, it's a crisis. As executives rely more heavily on information systems, their expectations about the reliability of those systems have taken a commensurate uptick.

"The average organization's requirement for recovery time from a major system outage now ranges between two and 24 hours. This requirement is pushed by the expectation an organization faces on all sides," says StorageTek's Martin. Customers expect supplies and services to continue—or resume rapidly—in all situations. Shareholders expect management control to remain operational through any crisis. Employees expect both their lives and livelihoods to be protected. Suppliers expect their revenue streams to continue. Regulatory agencies expect their requirements to be met, regardless of circumstances. Insurance companies expect due care to be exercised. The result? Instead of 24 x 7, people want systems up 24 x Forever, says Martin.

Disasters come in many sizes. When people think "data disaster," they think "major catastrophe"—an earthquake or a terrorist attack. But most often, it's the little things that hurt; the sprinklers go off, or a technician knocks the power cord out of a server. These small incidents won't close down an entire data center, but they will put a hitch in the proceedings. So when executives think about recoverability, they need to think at two different levels, says Scott Robinson, the CTO of Datalink. "If a server goes down in the data center, that's local recoverability. Remote recoverability is when the entire site goes down and you have to recover elsewhere." The challenge lies in successfully planning for both possibilities, he says. "The site disaster is bigger, but it's also far less likely to happen," he points out. "Hopefully, you build a plan and infrastructure that'll handle both types of events. Oftentimes, the systems built for one type of recovery can be leveraged for the other."

The different aspects of data protection must be integrated. Data protection involves a wide range of activities, from data availability to data recovery, all of which are key components of the business continuity plan. In the best of all worlds, each activity is integrated into a master framework and executed accordingly. But McAdam says that such seamless planning is generally found only at companies big enough to have a discrete group of people devoted to business continuity planning. "Generally, companies have different people responsible for different parts of the plan, and they just hope that those people talk to each other," she says. "Otherwise, the plan won't jell."

> **"Generally, companies have different people responsible for different parts of the plan, and they just hope that those people talk to each other, otherwise, the plan won't jell."**
>
> **—Diane McAdam, Illuminata**

Do the Analysis

Chances are, your company doesn't have the cash flow available to fund an entire business continuity department. And clearly, a jumble of isolated plans will not serve corporate data protection needs. So what's the best way to proceed? In order to build an integrated strategy designed to protect stored data and information—and ensure its continuing business value—IS executives should start by analyzing the different pieces of data security and protection involved. Once all the parts of the puzzle have been identified, it's easier to decide how they fit together.

Business continuity planning comprises a large range of issues, from factors involving the actual physical buildings of a company to emergency procedures and policies for employees to follow, says StorageTek's Martin. Building a secure storage environment, or data protection, is a third part of this discipline.

Companies often make the mistake of equating data protection with traditional backup. While the two are linked, data protection is more of a strategy, while backup is a component that provides the foundation for data protection strategies. Backing up refers to making a point-in-time copy of the data and moving it to some type of secondary media, which has traditionally been tape. Today's requirements demand that backup be augmented by other technologies that allow data to be recovered more quickly. For example, one such alternative is to use replication technology to make a copy of the data on a large RAID system.

Data protection is generally broken into two different areas: data availability and data recovery. Each part needs to be addressed, but each also presents different challenges when it comes to building an integrated data protection plan.

> **"Many companies spend months and months framing a disaster recovery plan but they won't implement it because the prospect is too daunting."**
>
> **—Tom Sylvester, senior director of technical services, Datalink**

Availability—This is the first line of defense in data protection; high availability refers to the practice of keeping systems up and running for a desirously long period. The gold standard for high availability is a system that has '5 nines' (99.999 percent) availability. It's a very high standard, however: '5 nines' availability translates into less than five minutes of downtime per year.

Achieving high systems availability is a top priority for companies such as financial service sector firms, where even a minute of downtime can cost millions of dollars. For example, William M. Farrow III, the executive vice president of the Chicago Board of Trade, says that he has little to no leeway when it comes to systems downtime. Traders at the exchange depend for their livelihood on the constant availability of systems such as his order routing and price relay systems. "I cannot go down," he says. "When we are trading, we are trading."

Executives like Farrow, a Datalink client, use several strategies to build high fault tolerance into their data architecture. The first is clustering, where two or more computers and storage devices are linked and configured similarly; if something happens to one, the other can take over. To business users, clustered machines form what looks like a single, highly available system.

Another popular practice involves the use of controlling software to replicate the data between two disk systems to make sure that each contains an identical copy of the data. This practice is known as mirroring the data.

Recovery—Data recovery comes into play once a system goes down. "It assumes that a service has gone away and needs to be brought back," says Datalink's Sylvester. Recoverability refers to how an IS department plans to get services back up and running, and data back in the hands of business users. Local recovery is used in the case of a relatively isolated mishap that doesn't affect the entire data center. System administrators can recover copies of the data locally and get it back in production while the rest of the corporate systems remain in service. Remote recovery is the heavyweight of disaster planning; it means that an entire data center has become disabled, and IS must reproduce the environment and recover all possible data using a remote site.

Build an action plan

Creating and maintaining a good data protection strategy is a tall order. Any plan must first of all satisfy the needs of the business, says Will Headapohl, the CIO of Gateway, a computer manufacturer (and Datalink client) based in Poway, Calif. "We identified first what the company strategy was, and tried to model our data protection plan on that strategy. We felt that was the right order of things, as opposed to building a data center and then building the business strategy."

But the strategy must also stay within prescribed budget targets. On top of all that, data protection strategies must flexibly mesh the differing requirements of each of the above areas of consideration, and in an ever-more complex business and technical environment.

Small wonder that many companies blanche at the idea, and stick their heads in the sand when it comes to data protection. "Many companies spend months and months framing a disaster recovery plan but they won't implement it because the prospect is too daunting," says Sylvester.

So how to start? With baby steps. Figure out what's most important, and protect that. Then work on the next bit. The decision doesn't have to be all or nothing, says Sylvester. One thing is certain, however: Companies that build no plan will find that nothing is precisely what they will be left with, should disaster strike. By following the agenda outlined below, executives will be able to draft a workable data protection plan that could save their businesses.

Analyze data for business importance. It seems hard to believe, but many companies spend more time worrying about what technology to buy than they do analyzing their business needs for storage. Sylvester recommends the opposite tack: "You've got to begin on the flip side and let business priorities drive the strategy."

Start by talking to business unit leaders, as they are the people who know which data are most vital to their business. "You can't have any kind of recovery plan without including the business side," says Rod Lucero, the chief architect of Conseco Finance in St. Paul, Minn. "They drive and map out what the important systems are."

Data generally gets divided up into two or three categories of importance:

Mission-critical data—This is the stuff that you can't live without; Amazon's website, or Bear Stearn's online brokerage system.

Critical data—This data is important to lines of businesses within the enterprise, and losing it will have an impact. However, the company won't hit the skids if it's inaccessible for small periods of time.

Non-critical data—It's nice to have this data if you can get it, but it's not strictly necessary (e.g. reference data that can be reconstructed from another source).

At Datex-Ohmeda, O'Brien's group segregates organizational production data from non-production data for the purposes of backup and recovery. Examples of production systems are ERP, email, logistics and finance; "These are the systems that we need daily access to," says O'Brien, a Datalink client. "These are the priority systems that we focus our backup, recovery and testing efforts on."

Conducting such an analysis can uncover some surprises, and it's smart to periodically revisit the exercise, as

Gateway

Gateway, a multibillion-dollar Fortune 500 company based in Poway, Calif., is a pioneer of the made-to-order personal technology industry.

Gateway's open systems infrastructure is built upon multiple SANs. The PC maker's dependence on e-commerce for business, as well as its manufacturing systems to custom build PCs in a very short period of time, means that it needs high availability from its systems and data.

Backup and Recovery

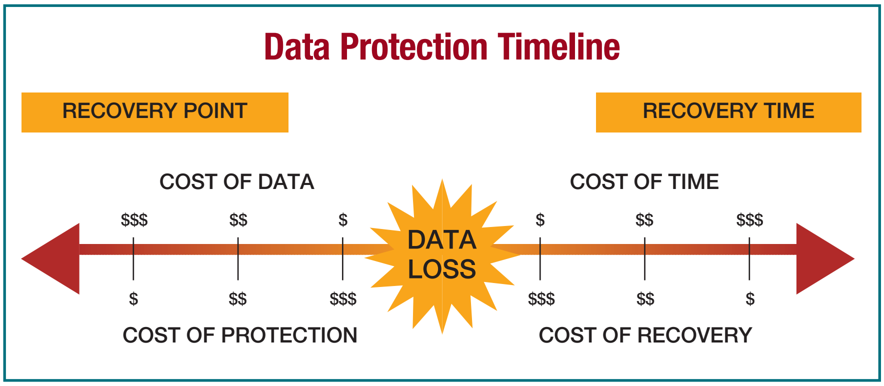
The company recently worked with Datalink to implement an exercise designed to prioritize and categorize its systems and data in terms of disaster recovery and protection. "We went through all our data and prioritized it as mission critical, desirable, and 'the rest,'" says Geoff Obeney, the vice president of technology infrastructure. "After we prioritized it, we were able to look at what storage technology we had in place and aligned the technology to the data based on those parameters." For example, the company's financial and manufacturing systems were deemed mission critical, and thus have highly available backup and remote mirroring in place.

Results

In terms of disaster recovery as a whole, Gateway's focused approach—which puts business goals as the basis for every storage decision—has paid dividends, says Obeney. "We've had less downtime, and fewer people standing idle," he says. "Given that we know the cost of downtime per hour per business segment, we can quantify the ROI, which has been significant. It has allowed us to reduce our IT budget."

data can wax and wane in importance. O'Brien, for example, says that his company has become aware over the past 12 to 18 months of the continual rise in email's importance. "It's more than just a replacement for the phone these days," he says, particularly since his company operates in several time zones. "It's truly a collaborative working tool, and that's the way we use it."

Do some risk management assessment. Many companies put the lion's share of their time and money into planning for large disasters, and they just might be betting on the wrong horse. "The vast majority of restores are single file restores rather than catastrophic recoveries," says Robinson. He advises that companies analyze the likelihood of a big disaster vs. the small ones, and make sure that they don't skimp on the small stuff. "If at some point you're considering a big ticket item such as remote mirroring or global clustering, you need to keep in mind those are for whole site disasters. Make sure you've built your system to cover the small—but far more likely—local disasters first," he says.



When developing a data protection strategy, you must consider both how much data you can afford to lose and how long it will take to get your data back.

Understanding the Nines

Here's What '5 Nines' Protection Really Buys You

99.999% uptime per year	5 nines	about 5 minutes of downtime
99.99% uptime per year	4 nines	about 50 minutes of downtime
99.9% uptime per year	3 nines	about 8 hours of downtime
99% uptime per year	2 nines	about 3.6 days of downtime

this includes both planned and unplanned outages

Map your recovery strategies and technology to the data.
To put this very simply, the most important data belongs on the most expensive technology—because the expensive stuff is generally also the fastest at recovery. For example, the data in a company's mission critical category may need '5 nines' availability, which means tape storage by itself cannot meet these needs. It will simply take too long to get the data back into production again. Protecting mission-critical data will generally involve a combination of technologies, such as data replication, clustering, or even a completely redundant data center that's updated in real-time.

Each category represents a different level of availability and recovery. By comparing the cost of lost business caused by data outage vs. the amount it will cost to get a system up and running, executives can arrive at a good balancing point for the two. Sylvester offers a hypothetical example. "Say an e-commerce website collects $25 million a day, and the cost to recover the site within 8 hours is $5 million. Depending on your risk tolerance, it may well make financial sense to pursue that strategy," he says.

Again, a great deal of input must come from the business side. At Conseco Finance, for example, Lucero says that the IS group will present business executives with the costs to recover a system in various windows of time. "We give them the windows of time and the costs associated with each, and let them go window shopping," he says.

Check for data interdependencies.
Once the data is divided into different levels of business importance and matched with a pertinent recovery technology, it's time to take a second look. The assignment: Make sure that the tier one applications don't depend for data on a tier two application that isn't backed up at the same rate. Otherwise, the scenario could play out like this: Your ERP system is mission critical, so

its information has been mirrored in real-time to a remote site. But the ERP system draws data from a small distribution system. The pipes are too expensive to mirror that system in real-time, so IS decided to back it up onto tape every six hours. The result: When the time comes to recover both systems, IS staffers will face the prospect of forcing six-hour old data to mesh with very current data. Not a pleasant situation, says Illuminata's McAdam. "One of the key questions I ask is whether there are interdependencies in the applications. If people say no, I say, 'Go back and look again.'" And once the inevitable is discovered, it's time to juggle the importance of applications and reprioritize until each application resides at the same level as the ones it feeds.

Remember that backup is not recovery.

There's no question that making a copy of all corporate data is a basic step in a good data protection plan. "Backing up data is like buying catastrophic health insurance," says Dan Tanner, senior analyst of storage and storage management at Boston's Aberdeen Group. "If something happens, you're covered, but you hope to hell it never happens."

But many companies assume that backing up data means that they are protected, and that's a big mistake, says Datalink's Robinson. Backup strategies are designed to provide file level protection and restoration capabilities, and typically backup architectures reside on the same site as the primary storage pools.

Obviously, because the primary and backup architectures are in the same physical location, if a business were to experience a disaster where the backups could not be accessed or the entire facility were destroyed, the backup data would be useless.

The bottom line is that "Backup and recovery are two different things," Robinson says. For example, say a company decides it can afford to lose one day's worth of data, and can afford to be down for one day. At the same time, the corporate recovery plan consists of nightly tape backups that are then sent offsite. That plan fulfills only one part of that equation. "If the tapes are going offsite it could take weeks to recover the data on them, so that plan won't answer the company's needs," points out Robinson. After all, he says, "Just because you have backed up a day's worth of data doesn't mean it'll take a day to recover it."

Top 5 Tips for Building a Strong Data Protection Environment

By Scott Robinson, CTO, Datalink

1 **Get executive buy-in.** Get it in writing if you must, but make sure that senior business leadership promises to be involved in the planning and implementation of a disaster recovery plan.

2 **Prioritize information systems in terms of business importance.** Figure out which systems are most critical to the business, which are less so, and identify the various databases, applications and supporting infrastructure that go with each.

3 **Weigh the cost of being down vs. the risk of being down.** Perform a business impact analysis to understand the costs of being down for each of those critical systems. Then weigh that against the risk of any one type of incident actually happening (e.g. a hurricane vs. an electrical plug getting knocked out of the wall). This helps you determine what you should spend on recovery technologies.

4 **Check for data interdependencies.** Some of the mission critical systems may draw data from secondary systems; your recovery strategy needs to take that into account.

5 **Test your plan.** Make sure your restore procedures work in real-time before you ever have to use them for real. And make sure that business users verify the integrity of the restored data.

In other words, building a solid backup strategy is just the first step towards building a good recovery plan. “A good recovery plan incorporates the right restoration architectures given the recovery time and point objectives of the business, by application,” says StorageTek’s Martin. “Therefore, a backup strategy is an integral component of a comprehensive recovery plan, but in and of itself, is not an entire recovery solution.”

Agrees Tanner, “You can’t recover if you don’t have backup, and there’s no point in backing up if you don’t have a good recovery plan.” Companies should have plans that address both.

To build those plans, Robinson recommends going back to that favorite business tool, the cost/benefit analysis. In this case, IS executives need to compare the cost of recovering the data they’ve backed up with the cost of doing business without the data. “You have to find a balance between what it costs to lose data and what it costs to recover that same data, and figure out how far on one side or another they need to be,” says Robinson.

So, for example, if a company wants its data recovered very quickly—and what company doesn’t—it can implement technologies such as a remote site that updates data in real-time, instant mirroring and frequent point-in-time data copies. Naturally, these technologies don’t come cheap—not as cheap as tape backup, for example. So CIOs find themselves weighing the cost of the recovery technologies against the value of the business data to be recovered, and finding a balancing point that satisfies both budgetary and business demands.

Pat Martin, StorageTek’s CEO, weighs in on availability and recovery

On the importance of building a data protection strategy: Business survival necessitates planning for every type of business disruption, from natural disaster to hardware and communications failure. While such disruptions cannot be predicted, they can wreak havoc upon the business if no strategy is in place.

On many companies’ vulnerability…

While many organizations claim to have a DR strategy, the majority of the strategies are unexecutable due to out-dated plans, lack of internal expertise, and inadequate testing processes. Organizations, especially those who depend heavily upon technology to operate, need to understand the costs of unplanned outages and weigh those costs against an acceptable risk management profile.

On how to integrate backup and recovery plans…

Understand where the backup architecture fits in terms of file level restoration needs. For example, if a disk platform is not mirrored and a file corruption or hardware error occurs on that platform, then a backup architecture could be used to restore the affected file(s). Additionally, for non-critical applications, a backup architecture could be used to supply the data to a remote electronic vaulting architecture to move the data offsite. The use of one particular technology or architecture is predicated upon the recovery time (RTO) and point (RPO) objectives defined by the business for each application used to support its business processes. RTO and RPO are usually quantified via a business impact analysis. With this understanding, the customer can make educated decisions on which architectures are required, and how to integrate the plans, while understanding the investment required and associated risks.

On the complexity of building a good data protection strategy…

With the growth of e-commerce and other factors driving system availability expectations toward 24 x Forever, the average organization’s requirement for recovery time from a major system outage now ranges between two and 24 hours. This requirement is pushed by the expectation an organization faces on all sides. Customers expect supplies and services to continue—or resume rapidly—in all situations. Shareholders expect management control to remain operational through any crisis. Employees expect both their lives and livelihoods to be protected. Suppliers expect their revenue streams to continue. Regulatory agencies expect their requirements to be met, regardless of circumstances. Insurance companies expect due care to be exercised. So the complexity is there, but it’s manageable as long as you set aside appropriate resources.

Take the plan for a test run.

McAdam at Illuminata tells the story of one customer she visited who had a very impressive 250-page disaster recovery plan. “I asked, ‘Did everything work right the first time you tested it?’ and the client got a funny look on his face and said, ‘What, you wanted us to test this plan?’”

In short, yes. It’s all very well to have detailed a strategy for protecting and recovering corporate data, but don’t wait until the data center is flooded to find out whether or not it works. And just one initial test isn’t enough, either. Data flows change, systems get reconfigured, recovery times can balloon as databases grow. “These plans still have to be tested six months and a year from now to make sure they still work,” say McAdam.

For example, Geoff Obeney, vice president of technology infrastructure at Gateway, says that they’ve tested their plan on an ongoing basis. “ These plans always need to be tweaked,” he says. “The first time we did it, we learned a lot. The second time less, and the third time even less.”

O’Brien agrees. Datex-Ohmeda continually conducts tests of tape backups to make sure that they work. “We want to make sure that we’re actually backing up what we plan to, and can efficiently recover it.” In the course of testing, O’Brien’s staff has uncovered some anomalies—areas of systems that weren’t being backed up as well as planned, or volumes of data that got moved to a different area and fell between the cracks. So as a result of the periodic testing, O’Brien’s staff has been able to identify areas for improvement and effectively manage it. And once again, Lucero says that it’s helpful to have folks from the business side review the recovered data to make sure it’s correct. ”The business people are the ones who know the data and know what it should be,” he points out. “We’re just the stewards.”

Look at how existing technologies can help you.

While newer technologies are undoubtedly faster at backing up and recovering data, they’re also more expensive. Companies can stretch their storage dollar further by taking an inventory of their storage products to see what forgotten gems may lurk in the data center hinterlands. “It always amazes me how much shelfware is out there,” says McAdam. “Companies might already have half the equipment they need. For example, many SAN software appliances can do replication from one site to another,” she says.

Think about calling in outside help.

As storage technology grows more complicated, so does the task of building a data protection and recovery plan. Lucero, for one, says that he’s found it helpful to get advice from vendor-neutral advisors such as Datalink as he’s implemented new technologies such as SANs and large new investments in disk storage. “They always bring to light what certain technologies bring to the table, without trying to push a certain manufacturer,” he says.

The past decade is littered with examples of companies that cleverly leveraged their information assets into competitive advantages. For one, the Ritz-Carlton Hotel chain’s store of information on frequent customer preferences has helped that company score a very loyal clientele. And then there’s FedEx, whose order tracking system knocked the stuffing out of the competition when it first debuted. Then there are companies such as Charles Schwab online, which literally built an entire business from electronic data. All these companies would never have achieved their successes if they were unable to analyze and draw conclusions from databases and files of business data. And storage is the common denominator that lets them do so.

It just makes good business sense to safeguard what has become one of the crown jewels of almost any Information Age corporation: corporate information assets. As stewards of the corporate systems, CIOs are in a prime position to provide a strategy to keep that data safe and available. And by creating and implementing such a strategy, IS executives can truly shepherd their company to a sustained competitive advantage. •

Last night there was a severe thunderstorm. But thanks to your relationship with Datalink, sunny skies were ahead.

First, we seamlessly integrated the StorageTek™ L700 and L180 Tape Libraries as part of your backup/recovery solution.

STORAGETEK™

Print

Which meant the proposal upper management worked on for so long was safe.

Leaving enough time to add the finishing touches.

Which put the client on cloud nine.

And you in a more temperate place. A remarkable chain of events, really.

datalink

Information Means The World.

866-213-1920 / www.datalink.com/cio