TAILORING DATA PROTECTION IS A BALANCING ACT

You're a star because you never drop the ball. On the data protection court that means matching up your data's lifecycle against a tailored protection solution to support it. And as your data's season wears on, its value to your company changes. So too must your strategy to defend it. Fortunately you have StorageTek sitting on your bench. Value, performance, results – you'll be wowing fans for years to come.

StorageTek

Storage

Enterprise-class data protection requires storage devices that safely and efficiently store and deliver data, day in and day out. This is true for every class of storage, from high-performance online disk to high-capacity tape libraries, or even vaulted tapes located far from your data center.

To validate your data protection strategy, evaluate its ability to hang on to that data. Where are you housing your various data sets? Is all of your most valuable data stored in enterprise-class storage devices? Is your least valuable data over-protected, and thus using up more than its share of your budget?

Management

Management typically takes the form of storage software, which helps protect your data ensuring that it is safe over time and distance, as it grows, changes and moves. It keeps track of what kind of data is where and why, so that it can be found, and accessed when needed. Media management, backup/restore, clustering and fail-over software are some of the components of intelligent management.

Starting with your most critical data sets, follow your information through its useful life and determine if it is being managed in a way that protects it from loss. Is it findable, movable and recoverable at each life phase? Does the speed at which it can be found, moved or recovered match business needs? Requirements vary throughout data's life; a new financial transaction, for example, and a three-year-old financial transaction are both important data that must be stored, but they have very different access requirements.

PRACTICAL DATA PROTECTION

Replication

No matter how safe and intelligent a storage system is, its ability to protect data will be limited by proximity. For the highest level of protection, data must be replicated in another location so that no matter what happens, it can be recreated.

How far away must your data be hosted to be safe? That depends upon the risks it faces. To protect against a hard drive failure, local mirroring will ensure that the data survives intact. To protect against damage or destruction of the data center, the data must be in another location entirely. Regional threats like earthquakes or hurricanes require even more separation. Look at your data and decide what risks you need to – and can afford to – defend against.

Backup/restore plays a role here, but remember that backups are not true copies. They are pictures of your data as it was at a moment in time. Your data is only truly copied by mirroring, with frequent updates to keep it current. This is a very expensive capability to implement and thus must be justified by compelling business needs.

Backups document history, but restores let you go back in time in the event of data loss. Verify if your backup/restore systems will allow you to go back in time as reliably, specifically, and quickly as required for each set of data. Backups exact a high cost in daily investments of staff, storage capacity and application availability. So your restore capability should be good enough to make that investment worthwhile.

Integration

Now that you've checked to see what storage components you have in place for each set of data you support, it's time to look at how those pieces work together to keep your data safe. There are two levels of storage integration to consider:

- Integration of store, manage and replicate elements into a solution on a per data set level.
- Integration of storage solutions on an enterprise level.

Per data set storage integration

Solutions are more than the sum of their components. Networking elements

INDUSTRY BUZZ

"Today's data centers are complex and data protection is critical. But all data is not created equal and all companies are not equal. StorageTek has expanded its family of data protection solutions to match data protection capabilities with data value and customer investment priorities. As they deliver these solutions over the coming months, StorageTek will be a company to watch."

– John McArthur, group vice president of Storage Research at IDC.

Fred Moore

President
Horison Information Strategies

Discovery: *What does tailoring data protection mean to you?*

Moore: Well, to me that means knowing the requirements of your business and what it takes to survive in case of a disaster. Whether you're a 7x24x365 business or if you operate six days a week or somewhere in between. The degree of availability your business requires will directly govern the way that you set up your business continuity and disaster recovery strategy. So, for example, airlines have continuous operations all year round, and they need to have the utmost data availability possible.

Discovery: *How should executives adjust their thinking on this issue?*

Moore: Some don't need to change, first of all. I think some people have implemented some very good strategies. But the "some" is far from all.

For mainframe companies, I believe the disaster recovery strategies are typically robust and very effective. But if those same executives are running a business that has based its computer architecture on Unix or Win2K or Linux, for example, then their challenge to implement a high availability DR strategy is much more difficult.

The Unix, Linux and Win2K computing platforms were developed to do computing and not to do too much with the data. It's a real mess compared to systems that were designed to deal with data storage from their genetic origins such as the AS/400 or traditional z/OS mainframe.

So executives' challenge is clearly more difficult and demands that they develop a centralized approach to storage management rather than permitting each department or entity to implement their own. Fortunately, the available storage management tools are finally improving in distributed environments to make this a reality.

Fred Moore writes an annual storage report that gives executives one-page snapshots of the hottest topics in IT, from technology to applications to networks to future trends. This year's Storage Manifesto *is available at Forum 2002.*

About Fred Moore

Mr. Moore is president of Horison Information Strategies, a consulting firm specializing in strategy and business development for emerging IT companies. He has over 21 years experience in the storage industry, speaking to worldwide audiences and publishing papers on the subject. He currently serves as editor-in-chief of Storage for West World Publications and serves on the boards of a few select storage networking industry companies. To learn more visit www.horison.com.

Michael Spotts

Corporate Evangelist
StorageTek

Discovery: *What does tailoring data protection mean to you?*

Spotts: I believe the insurance industry model is directly applicable to data protection. People buy policies to protect their personal assets-their houses and SUVs, for example, and they have a range of plans to pick from. The biggest insurance companies in the industry not only have a full line of policy offerings, but also tailor them to meet people's unique situations. This allows them to fit their protection with the value they want and at a price they can afford.

It's the same in the storage industry. Companies have assets they want to protect, that being their data, and those assets have different values at creation and additional changes in value over their lifetime.

Discovery: *Given that model, how should executives adjust their thinking?*

Spotts: Well, I believe that the big change in thinking that an executive has to realize is that all their assets don't require equal protection. You know, a kid at 18 doesn't require the same insurance as I do. I have more assets, more dependents, etc. That's the big shift. It's not an all or nothing approach, it's not a one size fits all.

So a company's data doesn't need the same insurance policy at creation or over its lifetime. When data is a "teenager," and gets tons of use, it's most valuable to a company and should have a policy in line with that value. That might mean using mirroring and other tactics. More expensive to be sure, but in line with the asset being protected. As the data ages, its insurance needs change as well.

I also think that when you look at the statistics relating to outages, disaster recovery/business continuance is but one of many risk outages companies need to consider. Naturally, September 11, 2001 brought DR to the forefront, and it should have. But I think that in day-to-day operations, companies need to look at protecting data against loss from the many other more likely outage possibilities.

About Michael Spotts

Mr. Spotts first began his 25-year IT industry career while serving overseas in the U.S. Army. He then served a 17-year stint with State Farm Insurance, working his way up the IT ranks and specializing in storage technologies in both mainframe and open systems environments. Mr. Spotts joined StorageTek in 1999, filling the role of corporate evangelist for emerging technologies. He keeps his hand on the pulse of business by working with customers around the globe to understand their challenges.