

Addressing the Roadblocks to Application Recovery through Integrated Recovery Management

EXECUTIVE OVERVIEW

Today's market challenges combine with the complexities of application management and recovery to create a difficult environment for IT managers. Compliance regulations and stockholders clamoring for increased security and decreased risks create the need for technology solutions to deliver increased recoverability while lowering costs of recovery. Integrated recovery management is a proven strategy for achieving the recoverability requirements of business managers while lowering IT and recovery costs across the organization and provide insight, protection and assurance related to critical enterprise data.

Application Managers

Pains related to recovery management

- >> Disconnected from storage and recovery strategies
- >> Unaware of application interdependencies

Introduction

There are a wide range of issues that impact application availability and recovery. However, the true nature of these challenges is not generally understood because of the siloed nature of application, data, and storage management. And with the slashing of IT budgets for 2009, many companies could choose to turn a blind eye to the problem – even if they found out their true exposure. The complexities of application management and recovery are often overlooked and masked by technology that is used in place of knowledge making companies unwittingly vulnerable. We believe there are four primary roadblocks to application recovery:

- >> The pervasive nature of applications
- >> The criticality of storage in application management
- >> The limited insight of the Business Continuity Professional into the IT environment
- >> The inability of executives and LOB managers to map the availability of their critical information with the growth and stability of their business


An integrated recovery management strategy can help address the requirements of these four audiences, and actually provide insight, protection and assurance related to critical enterprise data. The following pages outline the challenges we see related to these four roadblocks, as well as illustrate how an integrated recovery management strategy can reduce costs and drive business value.

The pervasive nature of applications

Applications are generally managed as individual components run by their specific functions or departments: AP/AR software, production or inventory management, customer service, etc. And while some ERP applications attempt to pull these functions into a common management platform, the fact is that few applications throughout an organization are specifically measured for long-term value related to their original acquisition and implementation costs as well as recurring maintenance costs.

The fact is that many applications – and their underlying architectures – become intertwined with the rest of the IT infrastructure like the wide roots of neighboring trees. The interdependencies of these applications, server, data, and storage resources are rarely fully understood. To be fair this applies whether an organization is server, mainframe/ server or mainframe based. All face the issue of lack of knowledge.

The tremendous exposure here is many-fold: data that is truly required by one application may be minimized during a manual Business Impact Analysis (BIA) process, causing that data to be allocated to Tier 2 storage resources, paralyzing the application that truly



required it. What's worse, strategic decisions regarding resource allocation, storage provisioning and data migration are made by management using rules that are consistent with managing storage not with knowledge of applications which further complicates the applications recovery.

One example would be tax tables that may be used by one part of an accounting package, but an application or recovery manager undermines its recoverability because they don't understand the interdependencies associated with that data.

The financial and retail industries are ripe with examples of ATM management challenges and branch office and remote store continuity exposures:

- >> In a proof-of-concept analysis at a global consulting, outsourcing, and professional services company, we discovered that more than half of their 50+ applications were NOT recoverable due to critical data not backed up. However, more than 90% of their backed up data was not critical. This greatly reduced their ROI on their legacy applications, and drove real risk that occurred on a daily basis in their production environment.
- >> A major financial services company with \$116 billion in assets was experiencing high backup costs due to replicating all production data across their environment. They recognized that replicating only their most critical data would reduce their backup costs related to disk requirements and management. A proof of concept analysis identified Tier 1 data that was being replicated, and should be migrated to tape with Tier 2 data, as well as Tier 1 data that was NOT being replicated and should be replicated to disk.

The criticality of storage in application management

It's true that storage resources are just part of the "supporting cast" in the application world – providing a repository for the data created and used by applications – but the real importance of data integrity as related to application availability is often too greatly minimized.

Organizations often treat applications, storage and disaster recovery management as if they are separate disciplines with separate goals when truly they should be working together toward the same goal. This separate thought process leaves many organizations vulnerable:

- >> Applications look at their data and their data only.
- >> The disaster recovery/continuity group looks at the issues of business operations recovery and data is only a portion of their overall responsibility.

Storage Manager

Pains related to recovery management

- >> Overspent on storage and redundancy because of perception that “more disk solves all problems”
- >> Treat all data the same without regard to application use
- >> Data volumes are growing and no clear strategy for allocation and management in place

- >> The storage management group manages data based upon management classes and storage classes many times without a full understanding of the applications and how their data placement decisions affect the overall recoverability of those applications. Restorable? Yes. Recoverable? Maybe.

Application owners are concerned that their run restart procedures are in place but their recovery strategy is generally not considered until the next test is on the horizon. Primarily, application recovery strategies are only approached from a single application owner’s perspective and without knowledge of how the application is physically being managed by storage management. The fact that they may have migrated data or they may have data that is on tape (virtual or physical) due to its size or use is not always understood by an application programmer. Even if the application programmer was aware, they generally would not know the specific technical details of how the data is actually organized and distributed. For example, monthly, quarterly, annual files commonly go looked over and this oversight undermines the entire recovery process.

Not to be overlooked, the single threaded process of recovering just their application doesn’t take into account cross platform and inter-platform dependencies. DR testing further entrenches this process since very few companies test all applications. Companies that replicate their data – whether complete or tiered – have application owners with a false sense of security and even worse senior management who believe the process is no longer necessary. True effort or resources given to the recovery process disappear.

In a best case, application owners conduct backups for their own individual application with no regard to other independent applications or data sets. They also do not consider point in time recovery needs or meet any specific RTO or RPO. This could increase the time required to conduct a live recovery test and lower its success rate and even worse, severely diminish the chances of a timely recovery in the case of a complete or mini disaster leaving an organization even more vulnerable.

Storage managers are always looked to if there is a problem with the application backups. “They must have the data somewhere” is commonly heard in the heat of an event. The problem with storage backups is that they manage data based on environment status – test, production and development – NOT by specific application names.

In this regard, storage managers do their job of maximizing the use of the storage that is on the data center floor. Though storage is “cheap”, it costs money to run and maximizing it with limited resources and staff is the storage administrator’s primary objective. Advanced storage strategies such as SANs and virtualized storage only complicate this issue – these technologies are great for reducing storage utilization, but they bring an additional level of management and tracking to the process.

The limited IT insight of the Business Continuity Professional

Continuity professionals are responsible for the entire process and depend heavily on their application groups and storage management to provide them with the knowledge that the organization is recoverable. Many do not have the knowledge themselves to ask the questions that would show the holes. They depend on conferences and vendors to inform them of what is acceptable and unfortunately these many times don't get deep enough to explore the "gotchas" or the information is from a vendor perspective.

More importantly, continuity professionals feel that the data component of the recovery process is the one area that has been worked on for some time and feel the need to work more intensively in other areas. Disaster Recovery/Business Continuity professionals often lack the technical knowledge to understand the nuances and many times don't know what questions to ask.

Application outsourcing also plagues organizations with more restorability issues. If storage is outsourced, the resources to manage data are based upon the outsourcer's stated practices that now have little knowledge of your data and its uniqueness. This puts an awful lot of responsibility into the hands of a person who manages data for many organizations, and many times is not even in the same time zone as the application owner. If you make any changes this is a change order and is very costly.

At no time does the outsourcer want to be responsible for the applications and if they are, they do this at a premium and still with little or no knowledge of the data itself. Interdependencies are overlooked. Volume level and change bit backups are all you will get and/or replication which as was stated above has its issues. In addition, outsourcers may outsource DR operations themselves and are typically not measured by RTO- and RPO- based SLAs.

If the application processing and hosting is outsourced, the new owners tend to keep the application in a steady state position. They now rely heavily on storage and technology to cover their lack of knowledge of how the application works and interdependencies are lost. Migration of data and data that is needed for monthly, quarterly and annual processing is assumed to be managed by storage and minimal thought is given to this area when recovery is involved.

Recovery Manager

Pains related to recovery management

- >> Not technically driven
- >> Static Business Impact Analysis are manually created, not often updated
- >> RTO/RPO set by business with no technology to back it up
- >> Overspend on redundancy to solve perception of recoverability

Business Managers/ Executives

Pains related to recovery management

- >> Needs to know exposures to downtime and customer satisfaction from availability
- >> Defined processes and auditing and reporting critical for compliance

The inability of executives and LOB managers to map the availability of their critical information with the growth and stability of their business

Compliance concerns continue to trouble organizations across every industry. These requirements do not go away just because the money available to fulfill them is not available. Cost containment is a must! The focus of many industries on data retention and security is certainly good business practice for customer service, patient health, and financial security – but it requires an integrated approach to storage management to ensure the auditability and reporting required to prove compliance.

The flip side however, is saving too much data just in case or with the thought it is easier and quicker because no one has to think about it. This approach may leave an organization open to litigation when data is saved when it was not required opening the door to discovery during litigation.

Recommendations: the unknown is the biggest threat

The challenge, then – after reviewing this short list of exposures to application recoverability – is to minimize the threats from unknown challenges. And since information is the key to providing insight, the answer can be found by continuously monitoring and reporting application and data use, providing real-time usage information about the application and its interdependent infrastructure of LPARs/servers, data, and storage resources.

There are certainly many tools and utilities from application, server and storage vendors that manage the I/O of their own resources; however, their siloed, proprietary view of their own hardware and software threatens to only aggravate the situation.

A holistic, neutral approach is needed to truly understand how to minimize these threats and break down the roadblocks to application recovery. We believe there are three imperatives to ensure application recoverability:

1. Measure “application value” in terms of the “ business value” it delivers

Large organizations that are decades-old and using legacy applications simply cannot measure the value of their applications by the capital or operating expenses required to manage and maintain them. Application value should be measured by the potential damages that would come from reduced availability or recoverability of that application. Lack of compliance with industry and governmental regulations carries fines and damages if applications and data are not available. And the loss of customers and brand equity from failure to maintain customer communications could shut an organization down forever.

2. Monitor and analyze data use by applications “in flight” in real-time

Lack of insight is primary cause of failure in any organization, from sales and marketing to production, accounting, and IT. You can't fix what you don't know is broken, and you can't identify exposures if you don't see the situation in real-time.

The only way to truly recognize the inherent value of applications is to know what corporate information it is using in real-time. This kind of “inflight analysis” provides the insight and information required to make a qualified decision toward ensuring application availability and recoverability.

3. Prioritize data storage strategies according to real world application usage

Too often organizations are driven to “save everything” in order to claim they are recoverable. However, too much data can be a larger exposure than many companies realize. Legal counsels know that any data that is stored beyond its requirements is still “discoverable” and requires ardent reporting and must be produced. And it simply doesn't make financial sense to buy more storage than you truly need – even with the decreasing costs of disk storage.

Tiered storage strategies are extremely cost effective if the right data is stored on the right media. It ensures that the most sensitive data is stored on resources that make it immediately recoverable. And less sensitive data can be stored on less expensive and less connected media. But tiered storage ONLY works when the storage protocol is based on real-world insight about how applications use data.

Integrated recovery management fits the bill

Integrated recovery management is a both a business model and a technology strategy that can minimize threats from data loss and lack of compliance, reduce costs related to DR testing and validation, and break down the roadblocks to recovery.

An integrated recovery management strategy starts with a complete monitoring and analysis engine that actively monitors application data usage “in flight” and analyzes its importance to the business. That data and analysis can be used by application, storage, recovery and business managers to determine the best storage strategy for that data, and helps measure “application value” in terms of the “business value” it delivers:

- >> Application managers benefit from:
 - Real-time insight into the availability and recoverability of their front-line resources
 - Critical data would be available on Tier 1 storage resources
 - Reduced chargeback from storage resource utilization

- >> Storage managers benefit from:
 - More intelligent decisions on storage acquisition, utilization and provisioning
 - Better use of strategic technologies like VTL, replication, etc
 - Reduced TCO of existing resources and better planning for new purchases
- >> Recovery managers benefit from:
 - Real-time insight into the availability and recoverability of their front-line resources
 - Better able to set and meet realistic RTO/RPO
 - Better use of outsourced recovery resources
- >> Executives benefit from:
 - Real-time insight into the availability and recoverability of their front-line resources
 - On demand reporting streamlines compliance audits

Conclusion

21st Century Software develops integrated recovery management solutions that provide midsize and large organizations with insight, protection and assurance related to their critical enterprise data.

Our powerful solutions provide valuable insight into how applications utilize vital data so that our customers can maximize the availability and recoverability of that information. 21st Century Software solutions optimize existing storage and backup strategies to better meet aggressive RTO/RPO requirements while reducing the costs related to recovery testing and actually extending storage resource ROI. And our customers can create reports and audits that provide documented assurance that their critical data will be available after any kind of event.

21st Century Software recovery management solutions are available for mainframe platforms, as well as Linux and UNIX open systems.

About 21st Century Software

Founded in 1992, 21st Century Software, has firmly positioned itself as a leader in the business continuity solutions marketplace, and has been solely dedicated to providing data protection and recovery management solutions to the Global 1000 marketplace. 21st Century Software distributes its products through its own sales channel in North America, as well as a distribution channel in Europe. Their DR/VFI product family was created in 1988, driven by the growing need of organizations to identify and recover their critical data and to integrate recovery management processes.

21st Century Software, Inc., 940 West Valley Road, Suite 1604, Wayne, PA 19087-1823
Tel. (800) 555-6845 | Email: sales@21stcenturysoftware.com | www.21stcenturysoftware.com

