Preparing for the storm: effective data backup and recovery

A Symantec Advisory Guide

Who should read this guide:
Functional IT management looking to increase the strategic value of IT as they implement a cost-effective and appropriately sized backup and recovery platform that can support business growth

Advice offered about:
- Overview of the backup and recovery landscape
- Insight into the latest technologies available
- Roadmap for advancing your current backup and recovery environment
- Real-life examples of how organizations have successfully re-architected their backup and recovery solutions
“This guide explores how organizations can use next-generation technologies and processes to deliver a more effective backup and recovery service.”

David McGowan
Senior Lead Technical Architect, Symantec Global Services
Preparing for the storm: effective data backup and recovery

How to use next-generation technologies to deliver a more effective backup and recovery service

Contents

Introduction ............................................................................................................................................. 4
Why are backup and recovery critical to the business? ................................................................. 5
Eleven signs that your backup and recovery environment may be inadequate ......................... 7
How to define your backup and recovery needs ................................................................. 10
Seven steps to a next-generation backup and recovery solution ........................................... 13
Case studies ...................................................................................................................................... 17
  Example 1: Large telecommunications company ................................................................. 17
  Example 2: Retail company ........................................................................................................ 18
Assessing next-generation backup and recovery solutions for your environment .............. 20
  Implementation planning ........................................................................................................ 21
About Symantec Global Services ............................................................................................. 22
Introduction

Backup and recovery are a particular concern for IT managers, who now need to handle larger and more complex volumes of data while reducing cost and increasing service to the business.

The backup and recovery process is becoming a major challenge for most organizations. IT departments face demands to provide a higher-quality backup and recovery service at a time when data volumes are exploding and budgets are being squeezed. Backup and recovery are a particular concern for IT managers, who now need to handle larger and more complex volumes of data as they reduce cost and increase service to the business.

Many organizations are simply not equipped to meet the backup and recovery challenge because they have outdated infrastructures. Their IT networks and systems cannot accommodate the increasing numbers of mission-critical applications that demand lower downtime. Nor can they deal with the complexity that arises from tailoring service levels to the needs of individual business applications.

“We commissioned this guide because we believe organizations need to start treating data backup and recovery with the strategic seriousness it demands. In our view, businesses that continue to reinforce their existing infrastructure, without consideration for backup and recovery, risk creating a financial black hole which consumes an ever-larger slice of the budget without delivering anything like suitable service.

“To help avoid such a scenario, this guide explores how organizations can use next-generation technologies and processes to deliver a more effective backup and recovery service.”

David McGowan
Senior Lead Technical Architect
Symantec Global Services

What you will get from reading this guide

- An overview of the backup and recovery landscape—and the challenges of controlling costs, raising service levels, managing complexity, and increasing accountability
- Details of new technologies to address the challenges—and provide the right level of protection to each area of the business
- A roadmap for improving your current backup and recovery environment—with a proven approach to mapping protection needs against technology options
- Insight into how other organizations are tackling this problem—with real-life examples of how global organizations have successfully re-architected their backup and recovery solutions.
Why are backup and recovery critical to the business?

The following demands combine to make backup and recovery a major challenge in today’s business climates:

**More data**
Mergers and acquisitions, coupled with organic data growth, are stimulating a steady increase in the volume of data that businesses need to protect. New disaster recovery, business continuity, and satellite data centers create still more data—as does the growth in mission-critical applications, at a time when consumers are placing more reliance on eBusiness.

**Need for faster recovery times**
Competitive and regulatory pressures are pushing IT to deliver higher availability as well as faster access and recovery for applications. In addition, more innovative, revenue-generating applications are being introduced, requiring non-disruptive business continuity that makes use of the latest operational recovery methodologies and technologies.

**Demands for better service**
As compliance and discovery requirements become more stringent and as IT risk management shifts from concentrating on IT operations to a focus on business strategy, backup and recovery requirements and data availability demands grow. As a result, IT faces ever more strict requirements for recovery point objectives (RPOs) and recovery time objectives (RTO)—requirements that must be met to avoid compromising critical business processes, violating service-level agreements (SLAs), and incurring the wrath of the business, its customers, and regulators. Further demands stem from government regulations, which force organizations to establish more robust data retention policies and procedures and to be prepared to demonstrate compliance with operational recovery service levels.

**Greater complexity**
The challenge of protecting so much information is compounded by the growing complexity of the supporting infrastructure. Information is now backed up and archived across multiple geographic sites and remote offices. Even within a single data center, there will be a variety of servers, storage, networks, and specialized applications and tools, each with its own user interfaces, policies, agents, and reporting technology.
Fewer resources
All of the preceding challenges must be met using staff, infrastructure, and financial assets that are already in high demand from other urgent and business-critical applications. Indeed, with IT budgets slowing or being reduced, companies that spend significant amounts on backup and recovery face the unenviable task of ensuring ongoing service improvements with fewer resources.

RPO and RTO
Figure 1 illustrates the two important measurements for backup and recovery performance. The RPO is the point in time to which data must be restored, and should be based on how much data the business can afford to lose. This is often considered as the time between the last available backup and the time a disruption could potentially occur.

The RTO refers to how much time a business can afford to lose as it waits for data to be recovered. It is based on how severely an interruption would disrupt normal operations and the amount of revenue that would be lost per unit time as a result of the lost data access.

Figure 1. Determining your data recovery needs.
Eleven signs that your backup and recovery environment may be inadequate

The challenges outlined in the previous section are real—and your ability to meet them can be compromised if your organization’s IT architecture is inadequate. Here are some key indicators that your backup and recovery environment needs modernization:

**Sign #1: Fragmented backup and recovery solutions**

Despite the technology to centralize backup and recovery operations, many companies still deploy multiple backup and recovery environments for reasons related primarily to legacy issues—for example, the need to separate UNIX and Windows®, provide for multiple solutions obtained through mergers and acquisitions, or wall off critical applications with their own infrastructure. Scalability issues with existing technology are another problem.

While each individual backup and recovery decision may well have been reasonable, the cumulative impact can be damaging. The results can include multiple tape libraries, increased numbers of backup servers, multiple enterprise backup products, and the need for multiple management teams. What’s more, these undesirable results have huge cost implications stemming from increased hardware and software expenditures, large numbers of backup administrators and operators, and excessive use of data-center space.

**Sign #2: Poor restoration performance**

Older backup and recovery environments are unable to respond to the need for faster recovery of mission-critical applications. Although a typical LAN-based solution using a tape library will often still suffice for most data sets, this configuration cannot provide the near-instant recovery demanded by revenue-generating or customer-facing applications.

**Sign #3: Lack of scalability**

Many organizations find themselves spending considerable amounts of money on high-performance tape drive resources, and then struggling to integrate and optimize them. The drives’ lack of scalability can lead to backup-window overruns, prompting further capital expenditures on storage. Furthermore, high-volume servers often suffer from excessively long backup times across LAN links, which are simply unable to meet the RPO and RTO requirements of many modern businesses.

Some organizations persist in using snapshot techniques and off-host backup for data sets that are not the product of high-volume, mission-critical applications and may not warrant such expensive high-end backup and recovery technology.
Sign #4: Over-reliance on tape-based backup
Far too many organizations are still either totally tape-based or making insufficient use of disk solutions. This means that they cannot take advantage of the more advanced features of their backup and recovery management software—nor can they use appliance devices that could help them better meet their data’s differing RPO and RTO requirements.

Sign #5: Excessive use of snapshot technology
At the other end of the spectrum, some organizations persist in using snapshot techniques and off-host backup for data sets that are not the product of high-volume, mission-critical applications and may not warrant such expensive high-end backup and recovery technology.

Sign #6: Isolation from IT support
Many organizations with multiple sites have dedicated IT equipment at each location, along with multiple small-scale backup and recovery solutions. This can be a costly and unreliable way to protect data, and it often leaves smaller offices with little or no access to local IT support.

Sign #7: Inability to support advanced technologies
Many of the best new technologies for businesses—such as virtualization and data encryption—require different backup and recovery approaches. Organizations without a sufficiently modern infrastructure may find themselves unable to deploy these technologies without considerable effort. This is an indicator their backup and recovery will be similarly challenging.

Sign #8: Low reliability
The pressure of data growth and budget cuts can drive down backup reliability, causing backup-window overruns and failed or missed backups. In addition to indicating an outdated backup/recovery solution, low backup reliability can eventually lead to financial damage and a loss of reputation for the business.

Sign #9: Lack of accountability
The constraints imposed by shrinking budgets demand much greater accountability from backup and recovery solutions. In other words, to justify expenditures on tape and disk devices, media, backup servers, and software licenses, IT must be able to measure quality and demonstrate effectiveness. Many traditional backup and recovery environments are unable to provide this business-level reporting.
Sign #10: Escalating costs
A continual rise in backup and recovery costs can be a sign of lack of sophistication in the technologies used. Organizations with a simple two-pronged backup approach—using only tape drives and disk replication—will miss many opportunities to generate savings by introducing new technologies that provide a better balance between price and performance.

Sign #11: Excessively high administrative overhead
If the approach to backup and recovery is not coordinated properly, then every addition to the backup environment generates additional complexity, which in turn demands further management efforts. For example, the addition of extra tape drives brings with it a need for more physical intervention to operate the drives, and that means more staff hours.
How to define your backup and recovery needs

As shown in figure 2, a well-functioning backup and recovery infrastructure must be able to support the varying demands of a wide range of applications. These include:

- Enterprise applications that require almost instantaneous recovery
- Intermediate value applications such as company Web sites and email
- Lower-priority enterprise intranets and employee portals, which can tolerate low availability and less stringent recovery requirements

Figure 2. Required recovery time and relative recovery costs of various IT systems.

Matching technology to criticality

The ideal is to develop a backup and recovery model that matches the right technology to the right level of criticality. However, this has not always been easy, because most solutions have historically tended to be clustered at the two extremes: At the high end are expensive mirroring, array snapshot, and replication technologies that recover critical applications without loss in minutes or even seconds; at the low end are economical tape backups that take hours or even days to recover the required data.

This means that there is a vast middle ground of application data that is too important to trust to tape-based solutions but not sufficiently important to justify high-end, expensive technologies.
Filling the gap

More recently, a set of new technologies has emerged to fill this protection gap, which means that the full range of price and performance is now covered. These technologies, as shown in figure 3, include:

- **Disk backup and virtual tape libraries (VTL)**, whose falling price and improved performance allow the architect to enhance or replace classic tape backup.
- **Space-saving snapshots and continuous data protection (CDP) solutions** that promise higher performance at reasonable cost for intermediate-priority applications.
- **Data deduplication**, which can cut network and storage costs dramatically, both for backup of remote sites and for systems in the data center.
- **Off-host snapshots and replication** using point-in-time copies that are then backed up to cut RPO exposure and disaster recovery risks.

Figure 3. Recovery capabilities and relative costs of different backup and recovery technologies.

With these technologies, it now becomes possible to allocate backup and recovery budgets to protect each data class appropriately. Figure 4 illustrates one way to balance the budget with RPO and RTO requirements.
Figure 4. Allocating spending on backup and recovery technologies.
Seven steps to a next-generation backup and recovery solution

Despite the technological advances in backup and recovery, deploying them in isolation produces a solution that is far from complete. Most important, simply deploying these technologies does nothing to reduce the cost, inefficiency, and complexity of coordinating and supporting a wide variety of disparate hardware and software. Without a strategic approach, you may simply swap one set of problems for another.

The goal should be a backup and recovery solution that maintains centralization and provides a unified operational recovery management framework across the full range of supporting technologies. Underpinning the classes of service should be a scalable infrastructure that makes optimum use of both disk- and tape-based hardware and delivers consistently high performance and reliability. Finally, the complete solution should be fully accountable, with the ability to demonstrate compliance against SLAs. Such a solution is shown in figure 5.

Figure 5. Components of a next-generation backup and recovery platform.
All of this does not have to mean the complete replacement of every element in an existing infrastructure, however. In fact, with the right approach, you can incorporate most existing backup and recovery into the new solution.

Reaching this solution requires you to follow seven steps:

**Step #1: Assess the situation**
The first step is to determine whether there is a strong need for change. Evaluate your organization’s current backup and recovery capabilities, identifying improvements that would more closely meet business needs, drive down cost, and boost quality of service. Assess the existing environment’s performance and reliability benchmarking it against industry best practices. Include a review of the hardware infrastructure, the supporting software tools, and the organization and processes used to manage the solution.

**Step #2: Create a service catalog**
Next, define your backup strategy in the form of a service catalog. This will require a perspective shift—from seeing the complete backup volume as one “lump” of data of equal value to seeing the volume as multiple chunks of data from individual applications with varying backup requirements. In fact, most of that data will probably need only the most basic protection, so you may need to focus only on the data associated with mission-critical applications. Now, quantify each application’s business value in terms of acceptable downtime, speed of recovery, and tolerable data loss. You will then be able to classify your operational recovery requirements into a set of well-defined service levels with measurable quality parameters.

**Step #3: Identify point solutions**
Once the service catalog is defined, you can then match data classes to the appropriate backup and recovery solutions. Specify what combination of disk-based technology (basic disk, shared disk, or VTL), snapshots (hardware, software, full, or incremental), software agents, and deduplication is required.
Step #4: Scope the core infrastructure
Underpinning the point solutions should be a scalable backup and recovery infrastructure that makes optimum use of both disk and tape-based hardware. The range and number of point solutions should indicate the scale of tape and disk resources that will be needed, as well as the required SAN and LAN designs, server specifications, and storage provisioning layouts.

Step #5: Design the management layer
The management layer is one of the most critical components because it provides a unified backup and recovery management framework. Processes, procedures, and appropriate reports must be designed not only to address ongoing administration, but also to provide business-level reporting on reliability, capacity management, and service-level compliance.

Step #6: Develop the business case
In order to win funding and buy-in from other stakeholders, you can build a very compelling return on investment (ROI) model by looking at the potential savings in both capital and operational expenditures that would accompany a move to a new backup and recovery solution. Comparing the net present value of these expenditures (as shown in figure 6) with the anticipated costs of meeting data growth and maintaining service with an existing solution should clearly demonstrate the desirability of the investment.
Step #7: Migrate the solution

Once a new solution has been designed, the challenge is to migrate from the existing infrastructure while maintaining service and reducing business risk. You can achieve a smooth migration through disciplined project management that works closely with the appropriate IT support teams and follows strict change management processes.

Figure 6. Return on investments for a next-generation backup and recovery platform.
Example 1: Large telecommunications company

The challenge
The company’s backup and recovery solution was fragmented. Individual application areas, such as billing, ERP, and Web services, were running separate dedicated backup and recovery solutions. This approach generated huge inefficiencies and duplication, as each application area was supported by its own backup and recovery software, operational team, and tape library. Accordingly, the company’s hardware, data-center, and software costs were far higher than necessary.

The solution
Excessive use of data-center space prompted the company to explore moving to a single backup and recovery solution that would be managed by one product and would direct all data to a scalable enterprise-class tape library. The solution would be based on a dual data-center infrastructure, and backups would be sent across inter-site links, removing all manual tape-vaulting operations.

The project began with a pilot phase—the migration of a single application—designed to demonstrate the potential for savings. The pilot was highly successful: The migration generated enough savings to pay for the library, the new backup servers, and the backup and recovery software—which built a compelling business case for the rest of the project.

At the heart of the ultimate solution was a core backup and recovery infrastructure designed for scalability, redundancy, and automated cross-site backup. The infrastructure consisted of an enterprise-class tape library and a bank of backup servers in both data centers, all managed by a single clustered management server spanning both locations.

The company’s servers and data were categorized into 16 application areas. Each of these areas was assessed for data volume, application architecture, and backup and recovery service requirements. A new approach was proposed within the centralized infrastructure, as well as a controlled migration path away from the current solution.

The approach was then executed on an application-by-application basis in line with site change-management processes and approvals by the service-acceptance group. Each new approach was validated and proven before the associated legacy solutions were turned off. No interruption to backup service occurred at any point.
Part of this transformation program was a new operational architecture, which included a new backup and recovery solution to replace the company’s prior simplistic approach of full daily backups across a very distributed set of hardware.

The results
The single, enterprise-class solution generated seven-figure savings, encompassing both capital-cost and operational-cost reductions. It moved the business away from a decentralized, fragmented operational recovery approach to a more centralized, service-driven approach.

Results included:
• Decommissioning of more than 20 tape libraries and associated drives
• Standardization of all backups and recovery operations onto one product
• Introduction of a single management team
• Removal of all tape vaulting

Example 2: Retail company

The challenge
As part of a major supply-chain renewal program, the company was replacing hundreds of aging, internally developed applications across a distributed storage infrastructure with 30 to 40 industry-standard packages and a centralized storage platform. Applications spanned the entire gamut of information technology, from business functions (such as merchandising, supply chain, and supplier management) and support functions (for example, file serving, email, HR, help desk) to customer-facing systems (such as CRM and Internet shopping).

Part of this transformation program was a new operational architecture, which included a new backup and recovery solution to replace the company’s prior simplistic approach of full daily backups across a very distributed set of hardware.

The solution
The company had already deployed enterprise-class libraries to support mainframe-based data. Since most mainframe tasks were to be replaced with open-systems functionality, the company retained these libraries to support the backup and recovery environment for the open-systems data. The company also deployed a SAN infrastructure to handle all of its backup and recovery operations. Enterprise-class directors were employed for disk access. A separate fabric, based on lower-cost departmental switches, was used for tape devices.
To accompany this hardware, the company carried out a thorough audit of data volumes and backup policies. The result was a core backup and recovery infrastructure that consisted of:

- A clustered management server
- A bank of high-performance backup servers, connected to both tape devices and the enterprise disk via the disk SAN
- A dedicated backup SAN for connectivity to backup servers and high-data-volume application servers—and implementation of formal rules for port connectivity and SAN topology
- A dedicated LAN for all LAN-based backup

The results

The implementation of a centralized approach generated £1.5 million in backup and recovery infrastructure cost savings. In addition, incremental techniques for the large databases were able to generate savings of an additional £350 thousand. The project succeeded in achieving a collectively lower cost of ownership.

Key benefits included:

- Greater agility supporting the rapid rollout of 40 new business applications over a one-year period
- Greater scalability to meet increasing scalability requirements, including those of new applications that grew to much larger data volumes than initial estimates predicted
Assessing next-generation backup and recovery solutions for your environment

Symantec Global Services helps organizations deploy reliable and cost-effective backup and recovery solutions—the result of unparalleled experience in assessing, designing, transforming, and operating major storage and backup and recovery infrastructures for global companies across a wide range of industry sectors. The experience gained from our wide client base enables Symantec to apply true best-practice principles, drawing on a thorough understanding of the latest technological advances.

Architectural assessment
Backup and Recovery Assessment is a standard service offering from Symantec Global Services. It is designed to review existing architectures and identify areas for improvement based on new technology options and best-practice approaches. The assessment addresses both the physical infrastructure and the applications being protected.

Applications are assessed in terms of data volume, business criticality, and recoverability. Symantec consultants work with application owners to determine their expectations regarding the impact of unavailability and the expected recovery time. Any site-wide policies of criticality and recovery are also considered. A service catalog is then proposed, producing a finite set of measurable service levels that can straddle all application requirements.

The existing core infrastructure is assessed in terms of its design, management approach, and deployed technology. Its capability to support the proposed service catalog can be assessed, and a subsequent gap analysis produced to highlight areas that require improvement. New technologies are investigated to address any highlighted shortfalls. These technologies are assessed for feasibility of deployment and likely benefit to the business. A number of point solutions, ranging from simple tape-based backup to advanced disk-based solutions, are typically identified.

The output from the assessment is a blueprint for a new or updated infrastructure. This may consist of a radical re-architecture, such as a migration from multiple environments to a single centralized solution that incorporates new hardware and/or software; or a collection of individual improvements that offer potential fast, short-term wins.

Backup and Recovery Assessment is a standard service offering from Symantec Global Services, designed to review existing architectures and identify areas for improvement based on new technology options and best-practice approaches.
ROI forecast

The re-architecture of an existing solution can be justified financially in terms of an ROI forecast. Symantec Global Services has extensive experience in creating compelling business cases for new initiatives. A standard model has been developed for backup and recovery that typically involves:

- Modeling the existing environment in terms of individual components (such as servers, tape drives, libraries, and software licenses) and operational costs (for example, hardware and software maintenance, people, media, and vault operations)
- Applying costs to each individual component and estimating the total cost of ownership (TCO) for the current solution over a three- to five-year period
- Identifying and costing all components in a re-architected solution and producing a similar TCO, also projected over three to five years, that can also include upfront implementation costs
- Comparing the TCO figures directly to generate a predicted ROI figure.

Implementation planning

Once the client has approved a new backup and recovery solution, a formal project needs to be defined. Symantec Consulting project managers have extensive experience in implementing major backup and recovery change programs both on schedule and within budget. These programs address hardware and software deployment, as well as formal acceptance and seamless, risk-free migration into a live service.

The ideal time for a re-architecture is often in tandem with a backup software upgrade, and this too can be factored into the work.

A typical project plan addresses:

- New hardware deployment
- New software deployment
- SAN, LAN, and storage tasks
- Integration with third-party applications
- Acceptance criteria
- Change management processes
- Maintaining the backup and recovery service during migration

Symantec typically works closely with the client during deployment—in fact, many deployment tasks can be performed by the client’s own staff. This level of collaboration promotes the development of a deployment plan that reflects a shared commitment between Symantec and the client.
Symantec Global Services offers deep technical knowledge and proven expertise to help clients manage IT risk, performance, and cost. Our consultants have helped IT teams from over 95 percent of the Fortune 500 companies enhance and maintain the security, availability, storage, and compliance of their information and infrastructures. With more than 1,000 consultants worldwide, we provide consulting services to clients in more than 60 countries and participate in more than 4,000 engagements per year. Our consultants average 15 years of experience across all major operating systems, storage hardware, and application environments.

More information is available at www.symantec.com/services.
About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.