


Realtime
publishers

The Shortcut Guide[™] To



Availability, Continuity, and Disaster Recovery

sponsored by

ARCserve®
More than Backup

Dan Sullivan

Chapter 4: Putting It All Together—Recovery Management Scenarios for Small Businesses to Emerging Enterprises..... 48

- Different Business Requirements Drive Different Solutions..... 49
- Scenario 1: Small Business Backup and Recovery 50
 - Easy to Use Backups 51
 - RPOs and RTOs 51
 - Disaster Recovery..... 51
 - Archiving and Data Life Cycle Management 52
- Scenario 2: Midsize Business and Remote Office Protection 53
 - Increasing Data Protection Needs 53
 - Protecting Remote Offices..... 54
- Scenario 3: Operational Management and Enterprise Backup..... 56
 - Encryption..... 56
 - Deduplication..... 57
 - Centralized Management 57
- Scenario 4: Data Protection in Virtualized Environments..... 58
- Scenario 5: Continuity and Failover 60
- Best Practices in Availability, Continuity, and Disaster Recovery 61
- Summary 63

Copyright Statement

© 2010 Realtime Publishers. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtime Publishers (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtime Publishers or its web site sponsors. In no event shall Realtime Publishers or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtime Publishers and the Realtime Publishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at info@realtimepublishers.com.

[**Editor's Note:** This book was downloaded from Realtime Nexus—The Digital Library for IT Professionals. All leading technology books from Realtime Publishers can be found at <http://nexus.realtimepublishers.com>.]

Chapter 4: Putting It All Together— Recovery Management Scenarios for Small Businesses to Emerging Enterprises

Throughout *The Shortcut Guide to Availability, Continuity, and Disaster Recovery*, we have explored how to address the business and technical requirements of data protection. Some of the requirements are obvious and apply to all organizations: restoring from isolated failures, for example, accidentally deleting a file, and recovering from catastrophic failure, such as a natural disaster that destroys a data center. There are also less obvious technical and business needs. For example, server virtualization is widely adopted for its ability to improve server utilization and help control costs, but it introduces additional technical challenges with regards to backup and recovery. Business strategies can also influence recovery management objectives. A move to improve customer service by providing longer periods of access to online data directly affects the cost and required resources of recovery services.

These and other considerations have been woven into both the business strategy discussions and the technical assessments documented in earlier chapters. In this chapter, we take a different approach and consolidate key recovery management issues according to business types and the special case of failover recovery. We will consider five scenarios. Each scenario delves into typical business and technical issues faced by particular types of businesses or technology use cases; in particular, we will consider:

- Small business backup and recovery
- Midsize business and remote office protection
- Operational management and enterprise backup
- Backup and recovery with virtual machines
- Continuity and failover recovery

These scenarios are not mutually exclusive. Some of the discussion of small business backup and recovery services may be relevant to midsize businesses, especially those with remote offices. Similarly, virtual machine recovery management may be relevant to all types of businesses, regardless of size. Continuity and failover is such an important topic that we address it separately, although we will touch on failover in other sections when relevant. We will conclude this guide with a summary of best practices in availability, continuity, and disaster recovery.

Different Business Requirements Drive Different Solutions

When it comes to recovery management, one size does not fit all. Business requirements will vary by industry and company size. Consider how different the needs may be in the following examples that highlight different industries:

- A financial services company may need 24×7 availability of recent transactional data as well as more historical reports. If systems are down or data is unavailable, basic operations could come to a standstill. A credit union customer could not walk into her branch office and make a deposit, for example. When core systems are down in financial services, you are essentially closed for business.
- A manufacturing company that loses access to its inventory management system may be able to continue to function at a lower level of productivity. Using a combination of phone calls to other parts of the plant and having runners check and update paper backup systems, the company can keep some level of operations in place for a short period of time.
- A real estate management firm might be able to operate at somewhat normal levels for a day or even two if their primary management systems are down. Office phones, personal smart phones, and a stop at the closest coffee shop for WiFi access will keep real estate professionals in the loop, at least with clients and colleagues.

These examples show the range of needs with regard to recovery management. Perhaps the most telling aspect of these scenarios is the one common theme: *ad hoc* solutions may work for some period of time but sooner or later core systems must be recovered. Recovery management is not an option; it is a requirement in business. What type of recovery management solution you implement will vary according to your needs.

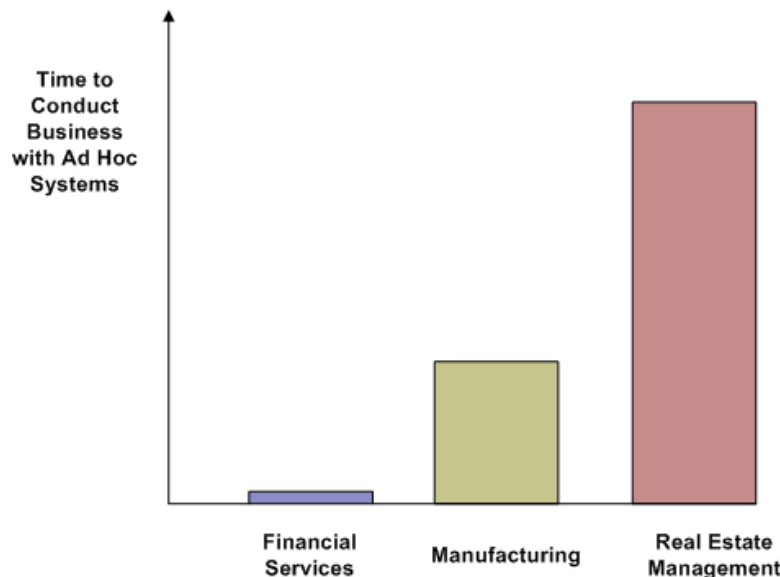


Figure 4.1: When data is lost or systems fail, it is only a matter of time before ad hoc solutions fail and business operations suffer significantly.

The notion of how long your business can operate without key systems is a helpful first step to understanding your recovery management needs. Thought experiments like this help get you into the right ballpark. To get the kinds of precise information you need to make business decisions, you have to delve into more detailed questions. In the next several sections, we will consider different business and technical scenarios and see how they influence a recovery management strategy. Across these scenarios, we will consider several key dimensions of recovery management, including:

- How long should it take to restore data and systems? These are commonly referred to as recovery time objectives (RTOs).
- What state of operations can we recover? This is known as a recovery point objective (RPO).
- Do regulatory compliance requirements impose recovery management requirements?
- How much data will have to be archived? How long will we keep it? These questions and others fall into the area of data life cycle management.
- How will we monitor backup operations and check the integrity of backups? These are operational issues within recovery management.
- What would happen if there were a catastrophic failure caused by a natural disaster? How would data be protected? Where would your business run critical operations? These questions fall into the area of disaster recovery management.

How you answer these questions dictates the type of recovery management solutions you will put in place. There is no one set of answers for particular-size businesses or for particular industries. A small health care provider may be subject to the same regulations as a large network of hospitals. A midsize construction company will likely have different recovery management needs than a similar-size retailer. In the following scenarios, we consider a range of examples that show how to understand the dimensions of recovery management, ask relevant questions, and discern the information about one's business that will help you understand the requirements of your business.

Scenario 1: Small Business Backup and Recovery

Mention the term “small business,” and you are likely to conjure up images of aspiring entrepreneurs filling niche markets while creating more jobs than their larger enterprise counterparts. Ask a small business owner what it is like running one of those companies and you'll probably get some of that positive imagery along with a healthy dose of reality. That reality includes a significant amount of time spent with accountants, lawyers, and bankers on top of the time spent on “real” work. Now add to the list the need to be the resident IT professional, and you can understand that recovery management might not get the attention it deserves.

Easy to Use Backups

One of the first requirements for small business recovery management is that it should not require a significant amount of time to manage backups. Small businesses, by definition, have limited staff. Automation and ease of use is a key factor. Backup software that provides agents for desktops, laptops, and servers can reduce the systems management overhead for small businesses.

In addition to easy-to-use software, small businesses should have easy-to-follow practices. If you have 10 desktop PCs and are installing backup agents on all of them, it is probably best to keep all 10 on the same backup schedule. That schedule should fit the needs of the most critical data. For example, the CFO's desktop should be backed up every night (at least). A good case could be made for not backing up as frequently the shared desktop used by part-time interns. After all, the data on that device is less important than the company financial data. The problem is that this strategy optimizes for storage space but increases the complexity of maintaining backup scripts and procedures. You now have two scripts to maintain rather than one. The savings in storage space is hardly likely to offset the extra management overhead.

In small businesses, a single, standardized backup schedule is better than many different ones. Larger businesses should classify their data and establish recovery management strategies based on different levels of criticality. For the small business, it is safe to assume all data is critical. (The one exception to this rule regards archiving, more on that follows).

RPOs and RTOs

Small businesses should define their RTOs and RPOs. If core business operations cannot continue without particular systems, those systems require short RTOs; financial services and retailers are examples. For other types of businesses, an RTO of several hours may be acceptable with next-day recovery conceivably sufficient for some low-demand systems.

RPOs address the question of how much work and data can be lost without adversely affecting the business. Weekly backups may be sufficient for businesses with relatively slow rates of change and those with comprehensive paper trails. In those cases, employees could re-enter transactions lost since the last backup. With advances in backup software, including ease of use and data deduplication technologies, it is probably a better idea to implement incremental nightly backups. There is not likely any marginal increase in the cost of backup software, additional storage costs are marginal, and the reduced risk is often worth those small, additional costs.

Disaster Recovery

A fire, flood, or other natural disaster can wipe out small business. If buildings are damaged, inventory destroyed, and paper files are lost, a small business could still recover. New office and industrial space can be rented and insurance can help cover inventory losses. Offsite backups may be the only way to recover important business records and transaction data.

Disaster recovery for a small business does not have to entail a complex set of data replication services and high-availability servers (although those are important for larger midsize and enterprise businesses). A simple strategy of keeping a full backup of all business data in a bank safe deposit box or other secure, offsite location can mean the difference between a disaster that sets back a business and one that breaks it. Cloud computing should also be considered. Cloud providers offer offsite storage that does not require you to transport, store, and manage physical media; as cloud services are available from any where with Internet access, your backups are readily accessible from virtually any location.

Archiving and Data Life Cycle Management

When it comes to keeping copies of data for long periods of time, you have to ask yourself what data is worth keeping. In larger businesses, the cost of data management warrants categorizing and prioritizing different types of data in the business. The high-priority and more critical the data, the more protection it receives. We noted earlier that small business should treat all business data as equally business critical in order to reduce management overhead. This keep-it-simple strategy can run into problems when we archive data for long periods of time.

The difference is that when we backup up data, it is written to tapes or disks on site. Both can be reused according to some schedule that meets data protection requirements. For example, tapes or disk space used for incremental backups can be reused once a full backup is made (assuming an RPO does not require the ability to restore to that incremental point). The goal of archiving is to keep a long-term copy of data, preferably in an offsite location in case of disaster. A practical consideration is how much storage media can be kept in an archive location, like a safe deposit box. Another question is, What is worth keeping long term? This is where the “treat all data as critical” rule of thumb breaks down for small businesses. Legal and financial professionals should be consulted on this question.

Archiving is a recovery management concern where we start to see some of the issues that midsize businesses have to address. Figure 4.2 shows a chart depicting the relative importance of various recovery management requirements to a typical small business. Of course, small businesses will vary in which topics they find important and this graphic is not meant to categorically describe all small business; however, it is useful for understanding the differences small businesses face when compared with midsize or emerging enterprises.

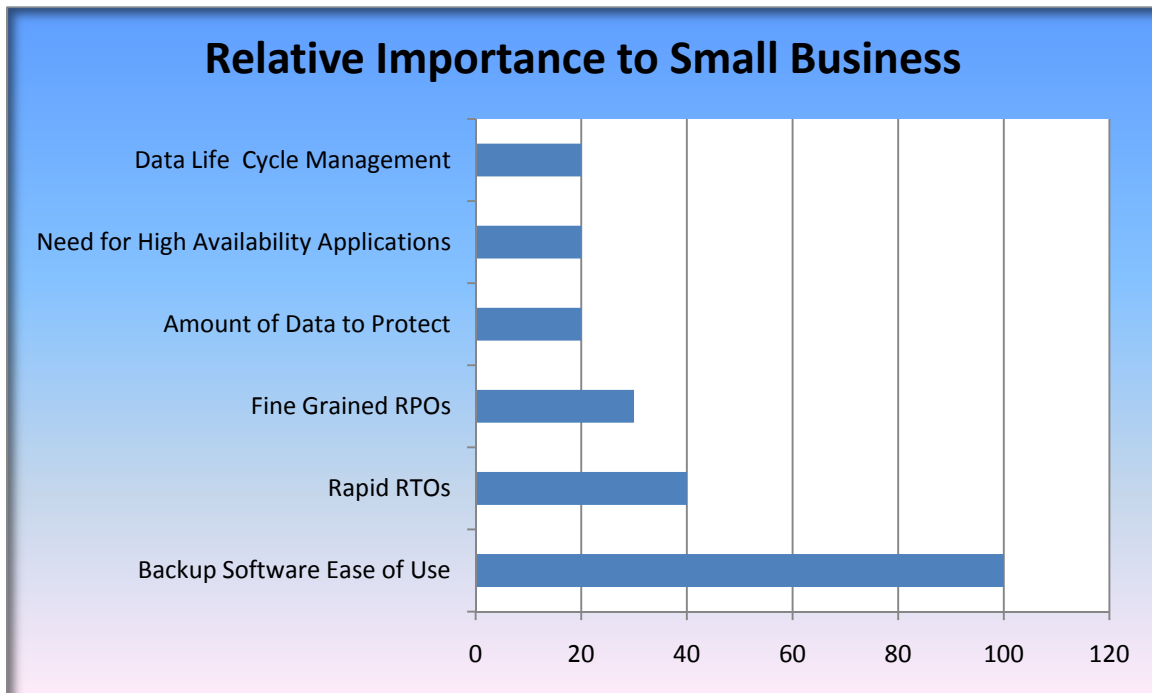


Figure 4.2: Top priorities for small businesses are ease-of-use considerations and the ability to provide basic data protection features.

Scenario 2: Midsize Business and Remote Office Protection

As companies grow in size, additional requirements move from the “nice to have” category to the “essential for business” category. Growing from small to midsize business tends to bring with it more demands on recovery management and data protection.

Increasing Data Protection Needs

In that way, a midsize business is more like an emerging enterprise with more risks to manage. In other ways, a midsize company may be more like small businesses in that they cannot support a substantial internal IT staff with deep and broad experience in a range of IT management and technical issues. This results in a typical set of requirements that is a mix of both small business and emerging enterprise requirements.

Ease of use, the ability to meet somewhat more stringent RTOs and RPOs, and increasing need for disaster recovery and more formal life cycle management procedures will be found in midsize companies. Another area of concern that midsize and larger businesses face is the need to protect data in remote office locations.

Protecting Remote Offices

Midsized and larger businesses often face the challenge of protecting data in remote office locations. Each of these remote offices can, in some ways, be considered like a small business. There are multiple devices requiring backup services but no dedicated staff to ensure data is properly protected. For the midsized business, there are a number of considerations with regard to remote office backups, including:

- **Consistency**—Businesses should have a recovery management strategy in place and it should be applied consistently across offices.
- **Cost control**—Duplicating backup servers across multiple offices can be inefficient. Remote offices may not warrant a dedicated backup server onsite; however, several remote offices sharing a single backup server can be cost effective.
- **Management**—Backup administrators need to have information about the status of backup operations. If a backup fails, for example because of insufficient disk space on the backup device, an administrator should be alerted. Management reports are also needed to monitor trends in time required to perform backups and the growth in backup storage.
- **Service delivery**—Restore operations should be done in ways that meet RPOs and RTPs. They must also be done in a cost-effective way, which means not requiring a systems administrator onsite at the remote location. Restores, like other management operations, must be done remotely. This requirement is especially problematic in those remote offices that have no IT staff, so such operations are passed on to someone else in the office.

All of these considerations can be met with a backup system that allows for remotely managed backups. Backup agents can be installed on remote office desktops and servers. The agents then function with backup servers in a central office to perform backup, restore, and management reporting operations. There is minimal need for onsite tasks, except for steps such as powering on devices. (Although this is less of a problem with remote management software that takes advantage of hardware that allows for network-based power-on and other basic management tasks).

The scenario depicted in Figure 4.3 assumes fixed, remote offices. In addition to these, midsized businesses should consider data protection for mobile users. We are far less tethered to our offices than we were even 10 years ago. Businesses do not need a dedicated office in a region to have a presence there. The US map in Figure 4.3 could easily become a global map if we were to include regional representatives for a midsized business who might be located in Asia, Europe, Oceania, or other regions of the world.

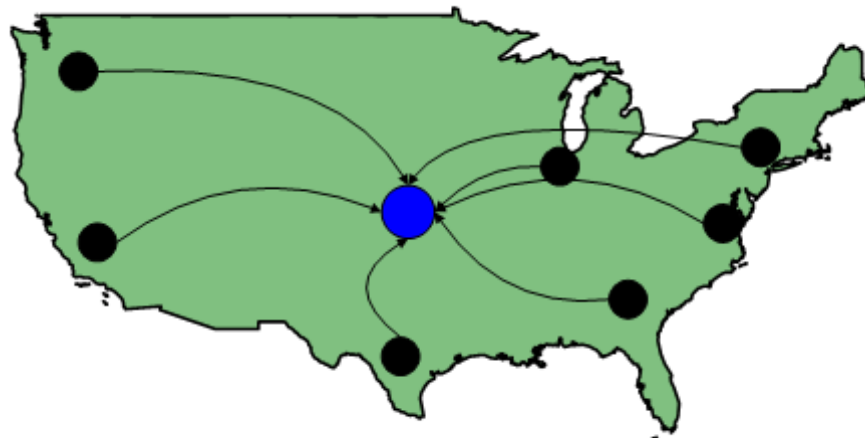


Figure 4.3: Remote offices should back up to centralized backup servers for efficiency, reliability, and manageability.

Note, when selecting backup systems to support laptop users, consider how often those users will have slow or unreliable Internet connections. Ideally, backup software will be robust enough to reliably perform backup and restore operations in spite of less than ideal connectivity.

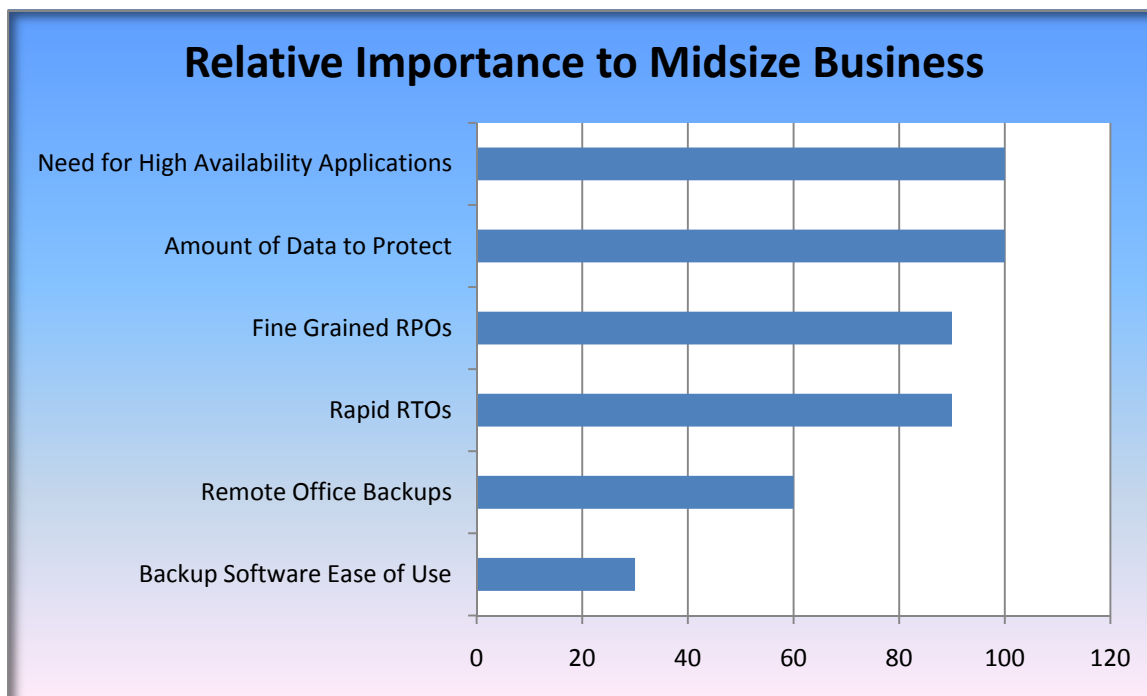


Figure 4.4: Top priorities for midsize businesses are similar to small business priorities but there is increasing emphasis on RPOs, RTOs, and amount of data to protect. Remote office backups become a concern for midsize companies.

Scenario 3: Operational Management and Enterprise Backup

Moving to larger businesses and emerging enterprises brings with it more complexities in recovery management and more diversity in requirements. Rather than try to capture a typical large business, we will consider three broad but common areas of concern:

- Operations management
- Data protection in virtualized environments
- Continuity and failover

Operations management in larger organizations includes virtually all the requirements found in small and midsize business but with different levels of importance. For example, there is less importance on ease of use when selecting backup software. This is not to say that ease of use is not important, it is; however, in large organizations, essential functionality must be in place even if it might not come with an easy-to-use interface. There are also features that become increasingly important as we move from small to midsize and emerging enterprises, such as:

- Encryption
- Deduplication
- Centralized management

These additional features are driven by a range of business requirements, including compliance, cost control, and the ability to meet service level agreements (SLAs).

Encryption

Encryption usually comes up in discussions about security. Discussions about transmitting sensitive business data over the Internet will quickly focus on encryption technologies to protect the confidentiality of that data. When businesses need to ensure confidential information is protected on laptops, even if they are lost or stolen, full disk encryption should be considered. Backups can share important similarities with these use cases and for those reasons, encryption can be an important feature of a backup solution.

Backups are often moved or transmitted to locations other than where the data originated. Offsite storage mitigates the risk of losing both a server and a backup to damage to a facility. Backup tapes may be lost or stolen while in transit. Security procedures at an offsite facility may be more lax than one would expect. In both cases, you have confidential data outside the protection of a business' normal access controls and physical security. Encrypting data on backup tapes and disks can provide an additional level of protection for ensuring the confidentiality of private and sensitive data. As a general rule, all business data that is stored offsite or in the cloud should be encrypted.

Deduplication

Reducing the amount of storage required for backups and the time required to generate backups translate into cost savings. Deduplication will be useful for any size business, but the larger the organization, the greater the benefit.

Deduplication can occur on either the source or the target system. Deduplication on the target side has the advantage of reducing demand on the source device's CPU. Backup agents do not have to support deduplication functionality on the client side when the operation is performed on the target. This can reduce problems with increasing the footprint of the backup agent on the source system. In addition, the target backup server can be sized appropriately to handle the computing requirements for deduplicating data from multiple source systems.

Centralized Management

Management features are important for any size business and any type of business. At minimum, you need to know that your backup processes run, your restores are successful, and the storage you have allocated for backups is sufficient. Management complexities increase quickly with the size of an organization, leading to several additional needs:

- Information about different types of backup processes, such as full, incremental, and differential
- The ability to define multiple policies for different classifications of data that require different backup schedules
- Reports showing trends in disk and tape usage as well as CPU utilization on backup servers
- Effective deduplication rates
- The ability to restore with minimal manual intervention, for example, not physically visiting a remote site to restore files

Centralized management affects how you perform backup operations, how you collect data about those operations, and how efficiently you can perform these operations. As Figure 4.5 shows, centralized management becomes one of the most important features of recovery management systems as the size of the organization grows.

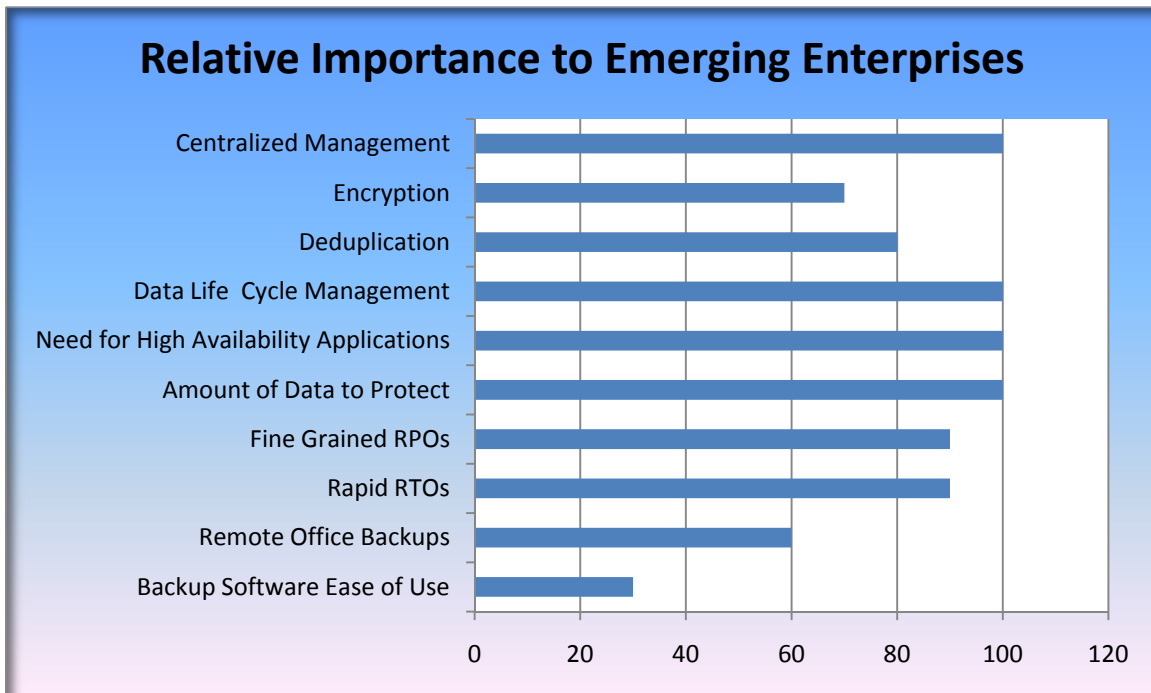


Figure 4.5: Top priorities for emerging enterprises expand beyond the set found for smaller business. Encryption, deduplication, and centralized management are important functions for larger organizations.

Scenario 4: Data Protection in Virtualized Environments

Server virtualization can significantly increase server utilization and help control hardware costs. There are, however, some recovery management considerations that need to be taken into account, especially for midsize and larger companies that deploy large numbers of virtual servers. Some of the most important issues are:

- Options for restoring virtual servers and files
- Demand on CPUs
- Integration between virtual machine services and recovery management software

Implementation details are important to understand when planning the use of backup software with virtual servers. Suppose you need to restore a file from a virtual server backup. Does the backup software support individual file restores from a virtual machine backup? If not, you will need to plan for additional time and storage space to accommodate the recovery operation. One way to handle the lack of selective file restores is to restore the entire image to a staging server and then copy the needed files to their target location. This process will increase recovery time as well as require additional storage space.

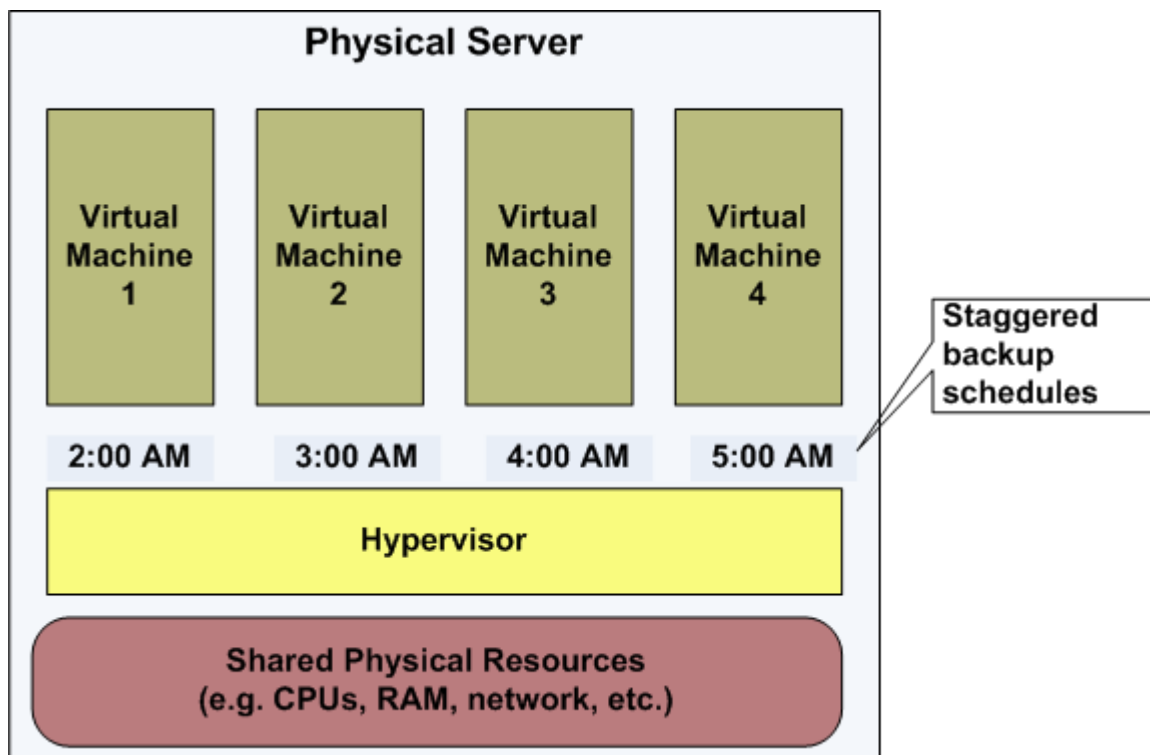


Figure 4.6: Backups should be staggered on virtual machines to minimize competing demands for shared resources.

Another implementation detail you need to watch carefully is the demand on CPUs during backup operations. Backups should not be scheduled to compete with each other or with other peak-demand periods on other virtual machines sharing the same physical server. Virtual machines isolate many management concerns to a single virtual machine, but backups are one of the areas where due consideration has to be made for global operations on the server.

Another issue to consider is how to maximize backup performance and available features by leveraging the features offered by the virtual machine vendor and recovery management software vendors. Each has specialty expertise. The virtual machine vendors can optimize low-level operations in the hypervisor, typically those close to the hardware, to increase performance. Recovery management software vendors are likely to offer more management functionality and provide a common feature set that hides some of the implementation details when dealing with virtual machines. Virtual machines are staples of day-to-day operations in midsize and larger organizations, but they can also play a crucial role in continuity and failover protection.

Scenario 5: Continuity and Failover

This chapter opened with a discussion of how different business requirements will drive different recovery management strategies. The question of how long and how well a business can function with systems down is a telling example of how wide ranging requirements can be. The ability to maintain continuous IT services increases in importance with the size and complexity of business operations.

Let's consider how a hypothetical midsize business might tackle the problem of disaster recovery. Our fictitious firm is based in the US with a headquarters in Chicago and regional offices in Atlanta, Boston, Houston, Denver, and Los Angeles. The executives in the business have determined that the company needs to be able to provide core business services even if the headquarters is hit by a natural disaster. The CIO and IT staff know five things they need to do to ensure a sound disaster recovery strategy and practice:

- Identify mission-critical applications and servers
- Define RTOs and RPOs
- Design a failover architecture
- Implement and manage recovery procedures
- Test the disaster recovery systems and procedures

Small businesses can reasonably assume that all data in the business is equally valuable and should be protected at the same levels. This is not necessarily true, but it is a useful fiction because it reduces the management overhead. As data volumes grow, the advantages of simplified management no longer outweigh the cost of maintaining unnecessary RTOs and RPOs.

From a disaster recovery perspective, mission-critical applications must have their data and servers protected in such a way that recovery times are short and recovery points are close to the time of failure. In our example business, management determines that the sales processing, financials, and customer relationship management (CRM) systems are critical. Other back-office applications, such as human resources applications, inventory management, and decision support are designated second-tier systems. They can be unavailable for up to 48 hours.

The sales processing system is accessible to customers through a self-service Web application, so management does not want customers to experience degraded service; that application will run on a dedicated server as well. Management also determines that they can tolerate some drop in performance in disaster recovery situations for other applications. The systems designers take advantage of this by running the financials and CRM systems, which normally each run on their own dedicated servers, in virtual machines hosted on a single physical server. The second-tier applications will run on a single physical server.

Designers decide to use the Atlanta and Denver offices as disaster recovery sites. The Atlanta office, like headquarters, has a dedicated IT staff, so it is chosen to host critical applications. Two servers are installed and dedicated to disaster recovery; one for the sales processing system and the other to host virtual machines for the other critical back-office applications. Denver does not have a dedicated IT staff, but they do have excess server capacity that can accommodate virtual machines running the second-tier applications.

To implement the disaster recovery plan, a high-availability application is installed in Chicago and Atlanta. Data is continuously replicated from Chicago to Atlanta to ensure RPOs and RTPs are met. High availability is not needed for secondary applications, so backups of those systems are copied from Chicago to Denver on a daily basis. In the event of a disaster, the Chicago IT staff will work with Denver staff to start virtual machine instances and restore the second-tier applications from backups.

The design seems sound. RPOs and RTOs can be met, business objectives are accounted for, and staff is in place to implement the plan as needed. Good disaster management strategies, no matter how well designed, should be tested. Things are bound to go wrong. Disasters tend to be, well, disasters, so you need to ensure that plans cover as many decision points as possible. Businesses should at least test at the unit levels that data is replicated from primary to standby servers, backups are reliable, and staff understand the procedures to follow in the event of a disaster.

Continuity and failover services are important parts of a recovery management strategy. Backup software and well-defined recovery procedures provide for basic disaster recovery services; larger businesses with more complex information management needs should consider high-availability and data replication applications as well.

Best Practices in Availability, Continuity, and Disaster Recovery

The *Shortcut Guide to Availability, Continuity, and Disaster Recovery* has covered a lot of ground in backup, recovery, and high availability. Sometimes we have delved into the technical challenges, other times we've looked at recovery management from a business perspective, and in some cases, we've tried to bridge the technical and business perspectives. As we conclude this shortcut guide, it is time to consolidate some of the topics we've examined and compile a summary of best practices in availability, continuity, and disaster recovery.

Best Practices: Making the Business Case for Recovery Management

- **Do not forget to address the obvious requirements.** Some of us in IT can get captivated by new applications, hardware, and methodologies to the point we risk losing site of basic business requirements. Remember, recovery management must be able to protect against basic risks: lost files, application errors, corrupted data, and catastrophic failures.
- **Account for expected growth in data volumes.** New business initiatives will create new demands for backup and disaster recovery. Make sure those needs are considered when assessing the feasibility and worthiness of new initiatives.
- **Not all data is created equal; not all applications are equally critical.** Do not buy more than you need when it comes to recovery management. Businesses face many types of risks without the need to eliminate all of them. Distinguish the value of different applications and types of data. Protect each according to their value to the business. Use risk management practices to inform your recovery management strategy.
- **Use data protection strategies to enable new business initiatives.** Recovery management, like other IT services, is not only a cost to businesses but an investment that enables innovative business operations. Give customers access to more data because you can keep it online for longer periods of time; open up analytic tools to customers to better understand their buying patterns because you can provide a reliable service thanks to replication and high-availability servers.

Best Practices: Overcoming Technical Challenges

- **Protect virtual servers and their data.** Backup and restore operations on virtual servers introduce new constraints not seen when dealing with physical servers. Ensure your backup software accommodates virtual servers, ideally providing the same features for both physical and virtual servers.
- **Understand application-specific requirements.** Relational databases, content management systems, and email systems all introduce challenges with restoring fine-grained data structures (for example, tables in databases and individual messages in email systems).
- **Support remote office backup and recovery.** Centralized recovery management can help control costs by minimizing backup infrastructure and reducing the need for IT support in remote sites. Also, accommodate laptop and other mobile devices that may not be continually connected to a corporate network.
- **Replicate critical data to a disaster recovery site.** Restoring from backups takes time. When continuous service is needed, use replication to keep a standby server up to date and ready to take over in the event of data loss or other failure. In cases where immediate recovery is needed, consider the use of high-availability applications that can monitor the primary server and switch to the standby server when needed.

Best Practices: Recovery Management Practices

- **Use the different types of backups, such as full, incremental, and differential to maximize protection while reducing storage costs.** Using incremental and differential backups can also reduce the time required to perform backups.
- **Use disk storage for performance; consider tapes when cost and portability are top priorities.** Disk-to-disk backups have speed advantages over tapes but tapes can be less expensive and are easy to transport to offsite storage facilities.
- **Understand data life cycle requirements.** Just as not all data needs equal backup protection, not all data needs the same level of archiving and preservation. Store backups and archives only as long as they serve a business need.

Summary

From small businesses to emerging enterprise, businesses are facing technical and business challenges to protect data and maintain continuous business services. Although there are not “one size fits all” solutions, there are sound practices for determining your business’ particular needs. Backup and recovery software has continued to evolve with technology. Backup solutions have adapted to virtual environments and take advantage of low-cost disk storage and changing business needs. These solutions provide centralized management consoles, consolidated reporting, and other tools to help IT staff keep up with increasing demands for data protection. Business practices have also matured as businesses leverage techniques such as remote office backups and practices such as managing data life cycle requirements to control costs without sacrificing data protection. Technology and business practices will no doubt continue to advance.

Download Additional Books from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this book to be informative, we encourage you to download more of our industry-leading technology books and video guides at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.