Data Center Strategies

In-Depth Research Overview

Survival of the Fittest: Disaster Recovery Design for the Data Center

Version: 1.0, Sep 10, 2007

AUTHOR(S):

Richard Jones
(rjones@burtongroup.com)

TECHNOLOGY THREAD:

Operations and Management

Conclusion

Business and market changes of the new global economy coupled with the explosion of digital media have made obsolete the traditional methods of tape backup/restore for corporate disaster recovery (DR). Advances in business continuity technologies, heavier reliance on information technology (IT) systems to meet competitive e-commerce needs, and regulatory legislation are forcing top executives to reformulate their DR solutions. DR planning is not insurmountable, however. Organizations can utilize new standards, methodologies, services, and technologies to create viable DR and business continuity solutions at marginal cost.

BURTON GROUP 7090 Union Park Center · Suite 200 · Midvale, Utah 84047
P 801.566.2880
F 801.566.3611
www.burtongroup.com

Publishing Information

Burton Group is a research and consulting firm specializing in network and applications infrastructure technologies. Burton works to catalyze change and progress in the network computing industry through interaction with leading vendors and users. Publication headquarters, marketing, and sales offices are located at:

Burton Group
7090 Union Park Center, Suite 200
Midvale, Utah USA 84047-4169
Phone: +1.801.566.2880
Fax: +1.801.566.3611
Toll free in the USA: 800.824.9924
Internet: info@burtongroup.com; www.burtongroup.com

Burton Group's *Data Center Strategies* service provides objective analysis of networking technology, market trends, vendor strategies, and related products. The information in Burton Group's *Data Center Strategies* service is gathered from reliable sources and is prepared by experienced analysts, but it cannot be considered infallible. The opinions expressed are based on judgments made at the time, and are subject to change. Burton offers no warranty, either expressed or implied, on the information in Burton Group's *Data Center Strategies* service, and accepts no responsibility for errors resulting from its use.

If you do not have a license to Burton Group's *Data Center Strategies* service and are interested in receiving information about becoming a subscriber, please contact Burton Group.

Table Of Contents

Synopsis

Global market reach (spurred by Internet e-commerce), fierce competition requiring just-in-time processes, tighter information technology (IT) budgets, explosive data growth, and new regulatory requirements have increased the importance of disaster recovery (DR) and business continuity planning (BCP). As a result, corporations are now under pressure to create, re-evaluate, and update their DR plans.

Research has shown that about 25% of corporations have insufficient or no DR plans in place.[1] More alarmingly, over one-third of corporations have not tested their DR plans in the past year. Recent regulatory requirements are now mandating that corporations have DR and business continuity plans in place. DR and BCP standards and certifications have resulted.

Almost two years ago, the International Organization for Standardization (ISO) published a new certification standard for information security, including disaster avoidance and business continuity. The ISO 27001 certification standard will most likely become a requirement for corporations to conduct business, following in the steps of other certification standards such as ISO 9001 for quality assurance. Corporate DR plans are best served by following the ISO 17799:2005 standard and seeking ISO 27001 certification of that standard for e-commerce and business-to-business (B2B) systems.

To meet the standards, technological advancements in data protection, replication, high availability, virtual machines, and business continuity solutions now offer newer and better methods for IT organizations. Explosive data growth has changed the landscape of data and system recovery, obsolescing traditional tape backup/recovery methods and demanding a new generation of technology to protect systems from disaster. Applying modern technology to DR and business continuity is not a "one-size-fits-all" proposition. Determining the value of each individual system and applying the proper level of technology ensures lower costs and higher efficiencies for DR solutions.

Internet technology advances, coupled with the explosion of co-location and hosting centers, offer additional advantages to corporations seeking to improve DR and business continuity. But co-location of business services is not for every company, nor for every system within the data center.

Finally, all top executives are well advised to drive the DR planning and ongoing maintenance processes within their companies. These executives must maintain constant vigilance over the business landscape, technological improvements, and new regulatory and competitive pressures to ensure their organizations are prepared for whatever may come their way.

Analysis

The birth and growth of the global e-commerce economy over the past decade has changed the way business is conducted. Global reach for suppliers and customers, explosion of digital media, competitive pressures for just-in-time manufacturing, resource maximization, and sweeping new regulatory requirements have shaped the business processes of today. Modern businesses have more need than ever to protect their viability in the event of calamity.

Disaster recovery (DR) is on the minds of most corporate executives who seek not only to avoid disasters, but also to ensure more rapid recovery should a disaster strike. Business continuity is a well-known industry term that refers to a corporation's ability to continue business instantaneously in the face of a disaster. In this report, instantaneous DR is synonymous with business continuity.

The Changing Face of Business

February 14, 2007, didn't bring heart-shaped Valentine's Day chocolates to the John F. Kennedy International Airport on Long Island in Queens, New York. Rather, a terrible ice storm brought the airport to a standstill. Passengers of low-cost airline JetBlue found themselves stuck for up to 10 hours in cramped airplane cabins on the tarmac. In just a day, the airport would resume operations, but for JetBlue, the ice storm was the beginning of a domino effect that would spell disaster for the low-cost airline and that lasted for almost a whole week.[2]

JetBlue, like so many other modern companies, is built on the premise of cut-throat low-price competition achieved through the combination of a slim, just-in-time workforce and aircraft equipment placement. A lean system with little to no overhead, JetBlue's just-in-time model works like a well-tuned machine, moving aircraft, pilots, and crew from airport to airport to maximize profits and lower costs. Maximizing aircraft flight time compared with ground time is the key. The ice storm on Valentine's Day disrupted the business machine; crew and aircraft were not available at other airports across the nation, flights were delayed, and more than 1,000 flights were canceled. The problem spread throughout the country regardless of weather. After a number of days, hoping the machine would re-synchronize itself, JetBlue was forced to cancel nearly one quarter of all its flights the following Monday in order to force its system back into synchronization. One week after Valentine's Day, the airline was back to normal operations. JetBlue estimated the Valentine's Day disaster cost the company $14 million.

JetBlue's Valentine's Day disaster illustrates new disaster scenarios that businesses face today. A number of recent events, changes, and influences are creating “the perfect storm” of issues that businesses must now deal with to protect from and to survive a disaster. For many organizations, existing DR plans are inadequate. The perfect storm consists of several elements:

- **A global market** has emerged in which businesses of all sizes now compete. Just one decade ago, only a handful of businesses had a global market reach. With the growth of the Internet and e-commerce, businesses of all sizes have been thrown into the global economy, competing for customers and suppliers over the Internet worldwide instead of locally or regionally. Unlike the past, when data-processing systems could be brought down on weekends for maintenance, or outages in the range of several hours could be tolerated, the e-commerce business model of today demands 24/7 data center business-application reliability and availability.
- **Just-in-time manufacturing and distribution** have reduced business costs associated with stock on hand. Competition between manufacturers and retailers squeezing every penny has become not only fierce, but also the norm. The Wal-Mart business model, in which stock allocations and sales revenue to suppliers are updated, calculated, and paid on a daily basis, has become virtually the only model by which retail business can compete in these times.
- **No-overhead operations** have forced companies to operate with slim workforces, and equipment that is allocated to nearly 100% capacity, nearly 100% of the time in order to remain competitive. These cost-cutting, profit-inflating methods demand intricate, detailed contingency planning in order to avoid chain-reaction events such as those that hit JetBlue.

- **Tighter information technology (IT) budgets** resulting from the tug-of-war between business operations and data-processing support have resulted in less money being available for IT operations. Rising fuel costs have increased the cost of raw materials, manufacturing, and distribution, pulling at corporate profitability (except for oil and gas companies, which have benefited greatly).
- **Natural and human disasters** have more than doubled in the past three decades. While debate rages as to the root cause, most scientists attribute the increase in natural disasters to global warming from greenhouse gasses (carbon dioxide emissions).[3] Furthermore, lack of planning on the part of electrical utilities is to blame for the 2001 rolling blackouts and the 2003 power grid failure.
- **Explosive data growth** has been fueled in part by the rapid move to digital media throughout all industries. Digital imaging, content, advertising, and communications (e-mail) have more than doubled corporate storage needs year over year.
- **New regulatory requirements** have driven organizations to both retain corporate data for longer periods of time and implement more advanced data-protection schemes. The Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), Basel II, Federal Rules of Civil Procedure (FRCP), and other similar regulatory requirements of the twenty-first century have only added to IT strain.

From the Top

Real life experiences teach the best lessons. Of companies that suffer an unrecoverable loss of critical IT data records, 43% never reopen, 51% go out of business within two years, and only 6% will survive long term.[4] Observation of those corporations that have successfully survived disasters teaches that all have one disaster-planning aspect in common: Disaster planning was driven and managed by top company executives. The chief executive officer and his or her direct executive staff must take ownership of not only the planning, but also ongoing testing and maintenance of the DR system within the company. Three reasons this must be so:

- Recent regulatory requirements have put legal “teeth” into the executive staff responsibility and accountability for disaster avoidance and rapid recovery**.**
- History has proven that executive involvement and control yields more successful plans and processes.
- Complete responsibility for the entire organization rests only with the top executives. Disaster planning requires whole-organization involvement, not simply the chief information officer.

While responsibility for disaster planning rests with the executives, they are not the sole knowledge keepers and will not be the sole executors of the process should the plan be called into action. All employees, including designated alternate plan executors, must be trained in disaster recovery.

Holistic View

Disaster planning includes all aspects of the business, its operations, and supporting systems. Successful planning includes:

- Human resources that are vital to a company's operations
- Physical facilities, utilities, backup power and cooling, and Internet service providers
- Supply chain/distribution channel planning with suppliers and alternatives
- Customer communication and support
- Data, applications, servers, desktops, network infrastructure, communications, and their configurations critical to business operations

Human Resources

The lifeblood of any organization is its employees. Businesses spend the greatest percentage of their expenses on human labor, making people the most important resource to a company. Employees are what make the organization function.

When Hurricane Katrina ravaged New Orleans, it left thousands of people disoriented and confused. While Katrina is an extreme example, it illustrates the importance of employee training. Employees need to know who to contact, and where to go to recover their lives and the business. Katrina further illustrates the sobering fact that human life may be lost, requiring contingent labor plans. Emergency operations center (EOC) plans can act as a homing beacon, calling employees to designated meeting locations to obtain information.

The primary function of an EOC is communication. Employee communication eases fears and speeds re-establishment of business processes. The EOC not only distributes information to employees, but also collects information, allowing for assessment of losses. Management is then able to mitigate organizational losses through reassignment of available resources.

Employee disaster training must be integrated into the new-employee orientation process as well as refreshed through DR testing with existing employees on an annual basis and when there is a DR process change.

Physical Facilities

Disasters damage the workplace, and in more extreme cases, completely annihilate the workplace. Even if the workplace is spared, disasters such as the New England power grid failure in the summer of 2003 take out utilities on which the workplace is dependent. Backup power systems comprising uninterruptible power supply (UPS) systems and diesel generator backup are expected core components of modern data centers, but can only supply power until the diesel fuel is spent. Plans should include methods of extending backup utility power in case of long utility outages. Furthermore, construction work down the street can accidentally result in cutting utilities or Internet service supplies to the workplace.

Alternate work sites that are geographically distant from the primary work site can be used to recover from this problem. But distance between the sites can be critical. In both the New England power grid failure and Hurricane Katrina, nearby cities were also affected. Residents and companies driven from New Orleans by Katrina significantly increased the burden on utilities and resources (electricity, water, Internet, and cellular communications) in Baton Rouge, Louisiana. Alternate sites should be located beyond the likely reach of a disaster.

Supply Chain/Distribution Channel

Suppliers and partners forge a critical link in business operations. In addition to communicating with employees, disaster-stricken organizations must include supplier and partner communications. Suppliers and partners must be included in EOC plans in order to obtain instructions to properly interact with the company during and after a disaster.

Suppliers and partners may also be victims of disaster. Redundancy in suppliers is good practice, not only to protect business operations from disasters that may strike suppliers, but also to ensure healthy competition among suppliers for the business.

Much like suppliers and partners, product distribution channels must also be included in the disaster plan, knowing how to contact and interact with the EOC in the event of a disaster.

Multiple distributors mitigate product-distribution risk if disaster strikes a distributor.

Customers

Customers are the revenue source for the company—the nourishment that keeps it healthy and growing. EOC communications plans include customer communications. Reassuring customers that the disaster-ravaged company is operational and fully able to support its customers is paramount. Customers appreciate the full truth coupled with planning advice in such situations. Inform customers of organizational functions that may be delayed in coming back online, giving them a timeframe. Corporations should plan to handle a spike in customer call volume and website hits as customers seek information about the company's operations.

IT Operations

The remainder of this report will focus on DR planning and technologies for IT systems and operations. IT systems include data storage, data protection, applications, servers, desktops, operating systems, networks, management tools, and system configurations.

Historically, simple tape backup of data met DR requirements for most organizations. Restoration involved restoring data from tape to server hardware. The protected data included application data, operating systems, the applications themselves, and system configuration information—everything necessary to recover the IT environment.

It's About Restore

Too often, IT organizations focus on system backup and not restore, pouring money and time into improving backup speed without regard to restore readability or performance. These organizations need to change focus and zero in on the goal: system restoration. Seemingly small mishaps can quickly become full-scale disasters simply because the restore process is nonfunctional or much slower than anticipated. The State of Alaska Department of Revenue found out the hard way. An IT systems administrator accidentally pressed an incorrect key, erasing the entire contents of a data volume. Moving to the tape backups of the volume, the Department of Revenue discovered to its horror that the tape backups were not readable. Their only recourse was to manually reenter the data, which took about 70 additional people for about one month at a cost of around $200,000 to accomplish.[5]

IT history annals are replete with similar horror stories of unusable backup tapes. Every IT organization needs to take a lesson from history and frequently test their DR processes, including recovery performance.

System restore performance or recovery time objective (RTO) and the amount of acceptable data loss or recovery point objective (RPO), not backup performance, are the metrics by which IT organizations must judge the effectiveness of their DR systems.

Standards for DR Planning

Information security management standards developed by the International Organization for Standardization (ISO) are outlined inISO 17799:2005. ISO 17799:2005 is a broad standard focusing on three areas:

- **Confidentiality of information.** Information must be protected by proper access controls and other security measures to ensure information can only be accessed by those with authorized access.
- **Integrity of information.** Data protection includes methods of protecting information from loss due to disaster, be it inflicted by Nature, Human error, or malicious means (such as virus attacks).
- **Availability of information.** Data and associated applications must be available to authorized users/systems without delays.

As an ISO standard, 17799:2005 does not enforce compliance. ISO 17799:2005 is simply positioned as a set of guidelines and best practices.

ISO certification standards, such as the ISO 9001 standard typically applied to manufacturing organizations, are well known in business. Along these lines, a certification standard, ISO 27001, was developed for the ISO 17799:2005 standard. The ISO 27001 certification standard was first published in 2005 at the time ISO 17799 was updated to ISO 17799:2005. The updates included the addition of a section covering regulatory compliance.

ISO 27001 outlines the certification requirements for the ISO 17799:2005 best practices standard in information security management. As a relatively new certification standard, ISO 27001 has not yet gained traction in the business world, but is expected to follow a path similar to the ISO 9001 standard.

The ISO 9000 family of certification standards for quality control were introduced in 1987, with updates made in 1994 and 2000. Today's ISO 9001 certification standard resulted from the simplification and combination of the ISO 9000 family in 2000.

ISO began tracking ISO 9000 certifications in 1993, which showed year-over-year growth. Certification counts revealed that ISO 9000 had grown in popularity to the point of becoming a requirement of doing business. ISO 9000 certification rose to the first item on the potential supplier evaluation checklist. Manufacturers lacking the certification found that they were not even being considered; hence the rush for manufacturing firms to obtain the certification began.

IT organizations can expect that ISO 27001 certification for e-commerce systems, including business-to-business (B2B) relationships, will most likely become a requirement for partnering in the near future. Executive risk-management needs will dictate the addition of the ISO 27001 certification to the company's portfolio. As corporations seek out B2B partnerships, they will desire a level of assurance that a prospective business partner has taken the necessary steps in policies and procedures to protect against disaster. As the industry recognized certification, ISO 27001 will become a veritable “credit score rating,” allowing corporations to put their trust in those business partners who have obtained and maintain the certification.

Corporations exploring ISO 27001 certifications should learn from the ISO 9001 world that applying the certification standard to all facets of the organization is not efficient. In cost-cutting efforts over the past five years, most ISO 9001-certified organizations have dropped certifications for internal corporate functions, only maintaining the 9001 certifications for direct customer- and partner-facing manufacturing and service processes.

The Value of IT Systems

The ISO 17799:2005 standard does not specify the technologies to be used for DR, but it does outline a process by which a system of policies and procedures can be identified, developed, implemented, tested, and continuously improved. Business IT systems are not all of equal value to the company, and likewise, the technologies employed to protect and provide for rapid recovery of those systems are not expected to be equal either. Likewise, disasters are not created equal.

A disaster is any event that significantly impairs business operations resulting in great financial loss. Restore of a lost or corrupted file is of a much smaller scale than restoring operations because of a site-wide disaster that destroys the entire data center. This report does not delve into the techniques utilized for individual file or object restores that are typically part of the day-to-day IT operations, but rather focuses on larger-scale disaster preparedness and recovery. However, many of the technologies and procedures for large-scale recovery may also be applied to day-to-day data recovery operations, which may range from accidental file deletes to file corruption due to user misuse of the system.

IT organizations should classify the value of their corporate systems and data based on the financial loss or threat to human life. The classification process is known as business impact analysis (BIA) and includes five aspects to determine system value: direct financial loss, risk to human life, regulatory requirements, dependent systems financial loss, and indirect financial loss.

Direct Financial Loss

Direct financial loss is calculated from financial loss-per-unit time that the system is unavailable. In most systems loss analysis, the rate of financial loss is neither linear nor equal for all systems. Take, for example an online order system. Internet web-based transactions will timeout within a minute or two, with automatic retry built-in to the web browser. In such a case, short delays in online transactions can be tolerated, and often not even noticed by e-commerce customers. As long as the transaction completes, short, infrequent delays in this example would represent no financial risk. However, longer system downtime creates business losses that can escalate exponentially. Conversely, in other industries, such as financial trading, a few seconds of downtime could represent thousands of dollars in lost stock trades. Figure 1 illustrates these points.

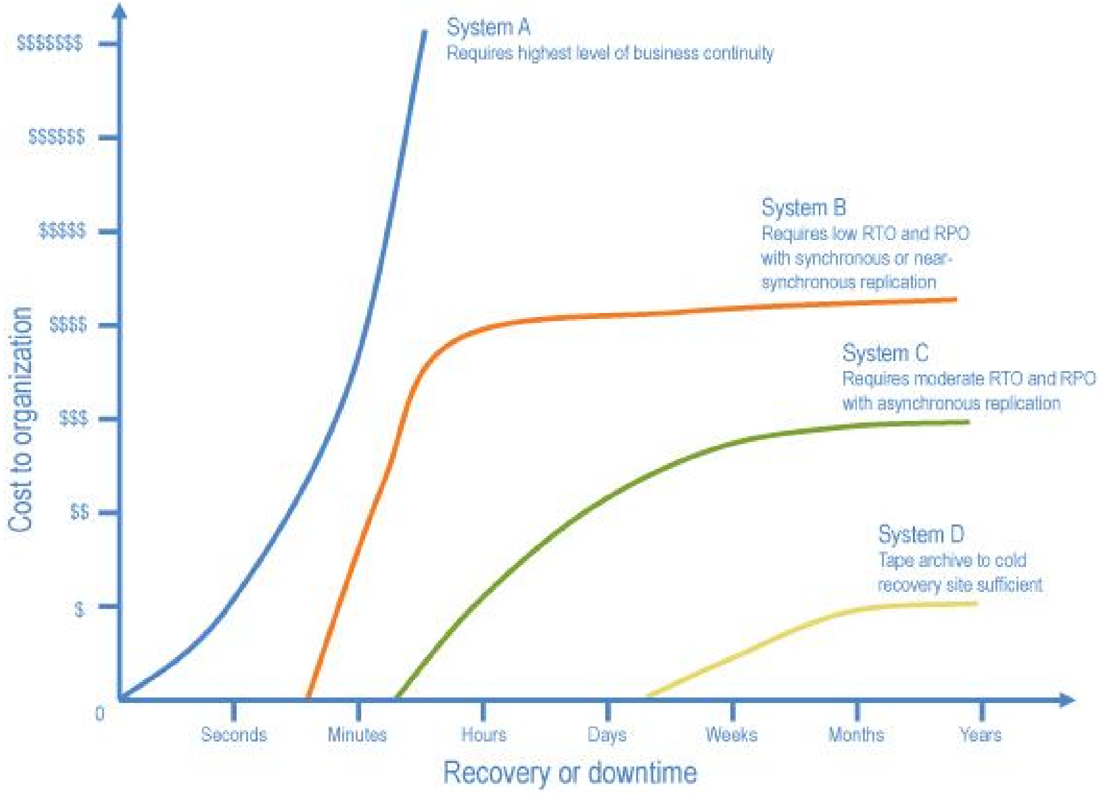

Figure 1: *Example of Financial Loss Potential per Time for Different Systems*

Risk to Human Life

Similar to direct business financial loss, system downtime in certain industries may present risk to human life and well being. Typically, these risks are not instantaneous, but over time may escalate and become threats to human life.

Regulatory Requirements

Business processes and systems that fall under regulatory controls must adhere to the law. At the time of this writing, regulatory requirements for system and data availability and recovery do not specify exact recovery timeframes. However, they do specify what must be recovered through data retention specifications. The two prior sections of this report define business loss as direct financial loss and risk to human life. Effectively, regulatory fines add to financial losses in the form of fines, legal expenses, and potential executive incarceration as the result of convictions.

Dependent Systems Financial Loss

Dependencies from secondary systems and processes will increase the total financial loss resulting from a primary system failure or outage. Short-term outages in primary systems may cause more catastrophic outages in secondary dependent systems, such as a financial market monitoring system failure that feeds an analysis system, resulting in misinformation and lost stock-trading revenue. Event chains may affect tertiary systems as well. Event chaining is an aspect of disaster planning that is often overlooked. Lack of event chaining planning is also a weakness in the ISO 17799, as called out in the *Security and Risk Management Strategies* overview, "Business Continuity Planning for IT." IT organizations should take care to thoroughly analyze all business systems and process dependencies and ensure a complete understanding of their cause-and-effect relationships. This information further serves to define the order in which systems must be recovered for proper operation.

Indirect Financial Loss

Loss of public confidence, either from customers or partners, due to frequent delays or short outages from system failures may be felt sometime in the future. Longer-term business disruption accelerates this effect. Typically, the "silent majority" (i.e., those people who do not express their dissatisfaction directly) will silently express their dissatisfaction by slowly migrating to competitors. These losses are much more difficult to quantify, but are real nonetheless.

System-Protection Continuum

Systems may be protected at various levels of recovery, both in recovery time and in the amount of system data preserved. Once the value of corporate systems and data has been determined, the RTO metrics are directly obtained from that analysis for each system. RTO is set by the corporation on a service-by-service basis, and indicates the time objective within which the service and its associated data must be recovered. Dependencies may complicate this analysis. For example, take Service A, which through analysis is determined to have an RTO of 30 minutes, and Service B, which is determined to have an RTO of five minutes. Dependencies show that Service B is dependent on Service A. Hence Service A really must have an RTO of five minutes or less, not 30 minutes.

Recovery of data not only includes a time element, but also a transactional element, which forms the basis of the RPO metric. Disasters strike at any time, resulting in system loss right in the middle of a data transaction. The data transaction cannot be completed in this case, and is lost. Recently completed data transactions, such as a newly sent e-mail message in a collaboration system, may not be protected by the system and may also become lost in a disaster. As a rule of thumb, immediately protecting completed data transactions is more expensive than protecting them sometime later. Fundamentally, this is the difference betweensynchronous andasynchronous replication. The value of the lost data transactions dictates the RPO that should be assigned to a system.

As the RTO and RPO metrics approach zero, the technology cost to achieve these objectives increases. A number of different technological approaches exist for achieving low to zero RTOs and RPOs. These can be categorized from asynchronous replication to synchronously mirrored redundant data centers withcontinuous data protection (CDP). Simple tape backup/restore is the least-expensive solution, but with relatively high RTO and RPO. Mirrored data centers prove to be the most expensive, achieving near or at zero RTO and RPO. Allocating the correct solution to obtain desired RTO and RPO metrics is paramount to containing costs in the data center. Figure 2 illustrates the system-protection continuum.

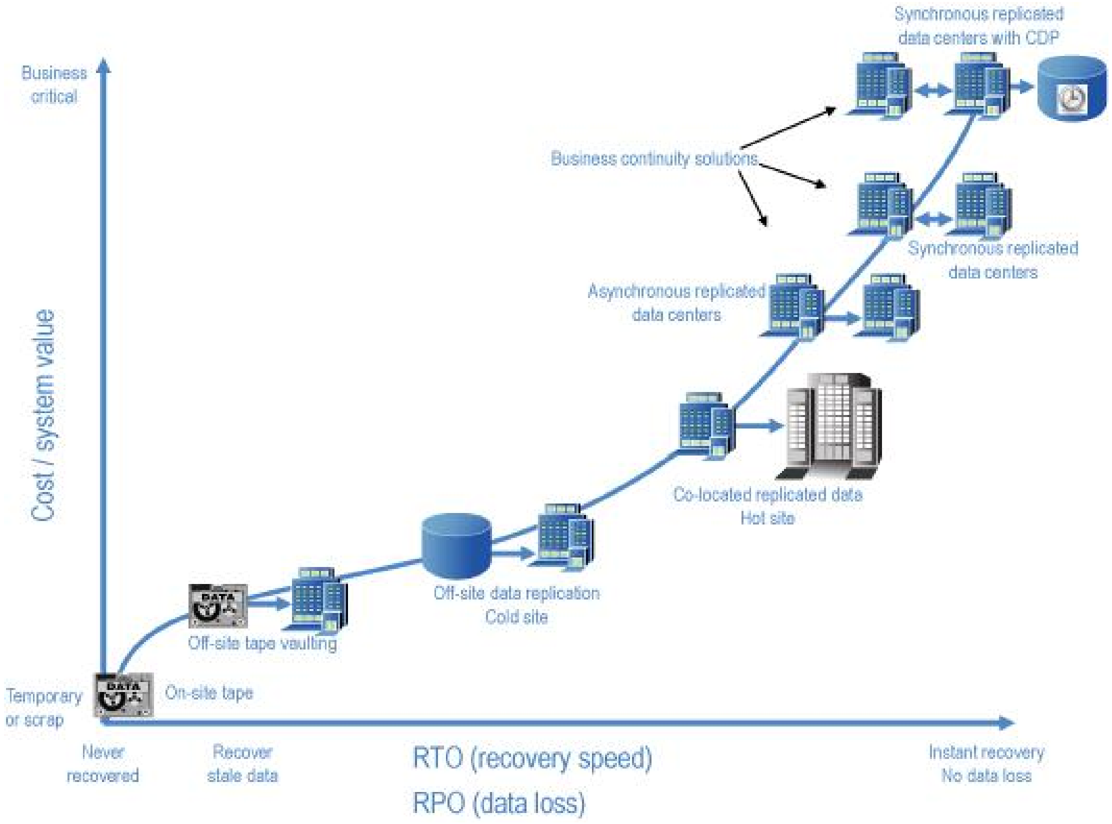
Synchronous replicated data centers with CDP
Business critical
Business continuity solutions
Synchronous replicated data centers
Asynchronous replicated data centers
Cost / system value
Co-located replicated data Hot site
Off-site data replication Cold site
DATA
Off-site tape vaulting
Temporary or scrap
DATA
On-site tape
Never recovered
Recover stale data
RTO (recovery speed)
RPO (data loss)
Instant recovery No data loss

Figure 2: *The System-Protection Continuum*

Tape backups kept locally in a data center offer no DR, as the systems and data would be completely lost in a site-wide disaster.

Mapping system and data value onto the system-protection continuum allows IT organizations to determine the best protection and recovery method at the lowest cost for their systems and services. The following sections describe these solutions.

Cold, Warm, Hot, and Business Continuity Sites

Various levels of disaster preparedness exist for DR. When disaster wipes out a whole data center, the business must reconstruct the critical systems and services of its data center in order to continue business. Alternate data center locations are classified as cold, warm, hot, and business continuity sites. Primary and alternate data centers are outfitted with UPS and diesel generator backup power systems that power the computer hardware, infrastructure hardware, and cooling systems:

- **Cold site** is a building or location with power and cooling but without server hardware, applications, operating systems, configuration, and data. The recovery time is long because the systems must be acquired, installed, and configured. Following which the data must be restored.
- **Warm site** consists of facilities populated with server hardware and supporting physical equipment, but no applications and operating systems have been configured. The systems must be configured and the data restored. Recovery is faster than cold site.
- **Hot site** facility contains installed and configured systems with current copies of applications and operating systems installed with near-current copies of the critical data ready to be brought up and configured. Recovery usually takes less than an hour.

- **Business continuity site** includes redundant systems that are configuration mirrors of the primary data center with asynchronously or synchronously replicated data. The systems are running; they are ready to take over within seconds. RTO metrics of less than a minute can be achieved.

Because of the global economy and greater dependence on IT systems today, almost all e-commerce business-critical systems require a business continuity level of DR, with RTOs of less than a minute. Less-valuable business data may continue to be relegated to cold site recovery, which typically takes about two weeks to recover. Data classified as scratch data would never be recovered.

Co-Location and Hosting

Co-location offers a number of advantages:

- Choice and lower costs as the result of competition from many regional and local co-location providers
- State-of-the-art facilities for cooling, power, and security as the result of competition
- High-speed, high-bandwidth, lower-latency Internet connections at discounted prices as the result of backbone proximity
- Business continuity sites (geo mirrored data centers) and DR planning offered as a service by many as the result of competition
- Lower RPOs at reasonable costs as the result of Internet backbone proximity (less latency and possibility to accommodate synchronous mirroring over longer distances)
- Mature co-location business models with service level agreements (SLAs) available
- Bonded for data privacy and security

Hosting providers offer an added service by supplying and managing systems hardware and software, which they locate in rented rack space of co-location providers. Hosting providers take on more of the IT responsibility for customers for additional fees.

Drawbacks of co-location are rarer nowadays, but may exist nonetheless. These may include:

- Poor choices available in certain regions
- May possibly cost more than existing facilities
- Organizations lack direct control over DR
- Not beneficial for non-web-based services such as file and print
- Co-location provider's mirrored data center may exist within the probable disaster effect radius

The Changing Role of Tape

For almost three decades, tape has been the mainstay of DR. However,tape technologies have been outpaced by hard disk drive technologies, leading to a problem faced by many organizations. While tape capacity has been doubling once every two years, HDD capacities have been increasing tenfold every five years. Growth of HDD storage coupled with the corresponding consumption of that added storage by expanding digital content has created the backup administrators worst nightmare: backups that do not complete in time. Restore times have equally elongated, which creates a critical risk to system disaster RTOs.

Disk-to-disk (D2D) backup/restore solutions, includingvirtual tape libraries (VTLs) have grown in popularity within the past few years as a method of solving the tape problem.

System Recovery

Operating systems, applications, and configurations must be restored prior to restoring the data. Failure to maintain accurate configuration information of operating systems and applications will result in failure to meet RTO metrics, or worse, failure to restore to a functioning state. Successful system restoration requires that IT organizations document and track all system configuration changes, including service pack and patch levels for operating systems, applications, and services. The ISO 17799:2005 standard mandates that organizations implement achange control system. Updating the off-site copy of the system configurationdocumentation and data must be a required step in the IT engineering change order (ECO) process. An organization lacking ECO and strict documentation discipline once suffered a disaster, losing a Microsoft Exchange e-mail system. The IT organization recovered the system and data, only to find that the recovered Exchange application repeatedly reported the data as corrupt, failing to recover the database redo logs. Another day of troubleshooting revealed that a later service pack had mistakenly been installed on the recovered Exchange application, rather than the service pack that had been running on the destroyed system. Backing out the later service pack allowed the Exchange e-mail database to properly mount for system operation.

Image backup and restore of the system volumes will ensure that application and operating system configurations are maintained. IT organizations must ensure that the ECO process includes updating the system image backup any time a change is made, along with properly documenting the current image. The correct image must be easily identified during a DR scenario.

Virtual Machines

Virtual machines offer the newest technology for DR with many lower-cost advantages. While these technologies are relatively immature, the promised improvement in manageability and lower cost has created a “gold rush” to virtualization. DR benefits of virtualization include:

- Virtualization results in hardware savings at the DR site by virtual machine aggregation of only critical services, requiring less hardware
- Virtual machine technology enables rapid hardware reprovisioning where test systems in virtual machines can be quickly shut down and recovery virtual machines quickly started
- Virtualization allows simplified synchronization of configuration changes to critical systems and services between primary and recovery sites
- Virtual machine image files simplify the tracking and management of system configuration changes to ensure correct configurations are recovered
- Virtual machine rapid DR management tools are available such as VMware VirtualCenter

Virtual machines are more efficient for rapid DR and business continuity if the systems at the primary site are virtualized. Physical to virtual migration during a DR takes longer to accomplish.

Full details on virtual machine options for data protection are covered in the *Data Center Strategies* report, “VM Backup Bliss? The State of VM Data Protection in the Enterprise.”

Business Continuity Solutions

Systems that require low RTO and RPO require geographically separated, actively mirrored, complete data centers: geo-sites. Geo-sites require that servers, applications, and data be continuously synchronized between the two sites. Stretch clusters, cluster-of-clusters, and virtual-machine management products provide these solutions. Each of these solutions has advantages and disadvantages. Figure 3 illustrates the stretch cluster approach to business continuity.

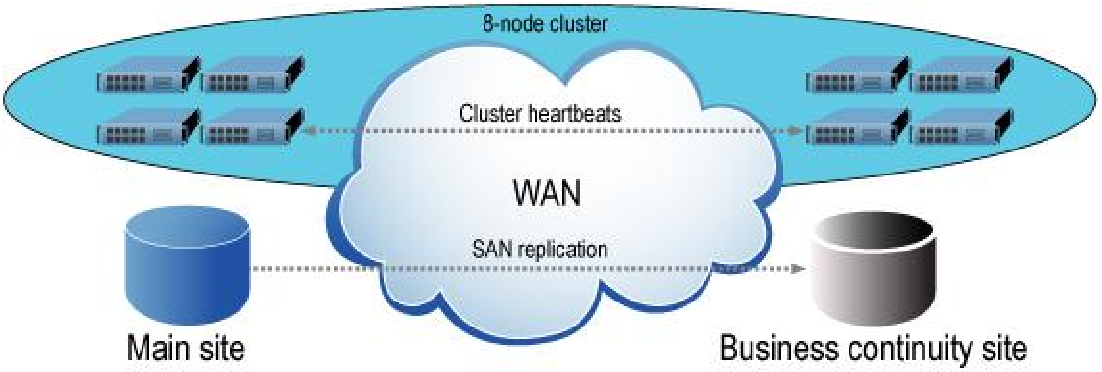

Figure 3: *Stretch Cluster Business Continuity Solution*

Advantages of stretch clusters include automatic failover of applications and resources between sites should one or the other site be compromised. Additionally, existing high availability (HA) failover clustering knowledge and training can be leveraged by IT staff in developing and managing failover policies within the stretch cluster.

Disadvantages of stretch clusters include false site failover events resulting from interrupted or broken wide area communications links. Additionally, special tuning of the HA cluster heartbeat timing parameters is required to adjust for the propagation delays introduced in the wide area communications links. This results in slower resource failover times within and between the two sites. Furthermore, DR planning typically requires that a protocol of tasks be followed at the point at which a disaster is declared, one of those tasks being to failover the services to the remote site. Automatic failover of services at the time the primary site is destroyed may result in more difficulties restarting the business processes at the alternate site as employees or other systems may not be ready. In such cases, manually initiated failover from the EOC at the proper time in the disaster sequence plan is required.

A better solution would be a cluster-of-clusters approach (see Figure 4), which would enable entirely different policies, parameters, and processes to be applied to each level. The HA cluster within a site would include automatic failover with rapid timeouts. The two sites would each be treated as nodes in a greater cluster that spanned the sites. This greater cluster would incorporate increased timeouts for automatic resource failover, and manually activated resource failover for those resources that can only move at the step required as part of the execution of a disaster plan.

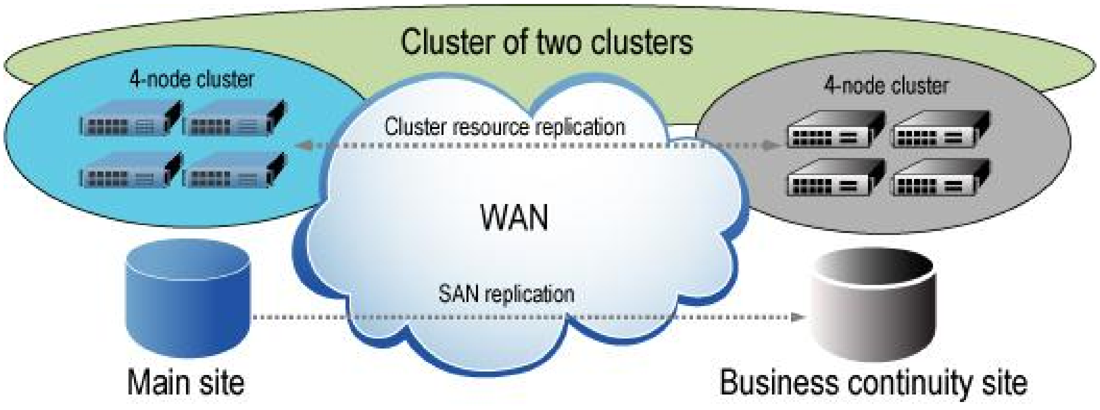

Figure 4: *Cluster-of-Clusters Business Continuity Solution*

Virtual machine management using VMware's VirtualCenter improves the ease of configuration and ongoing management of business continuity solutions. Server and application configurations are elegantly maintained in virtual machine images and virtual hard disk files. These image files are more easily managed and replicated from the primary site to the business continuity recovery site.

VMware's VirtualCenter for DR allows layering of its virtual machine failover control with third-party HA clustering solutions, effectively creating a cluster-of-clusters. This allows for the multi-level control needed to meet local and global service availability needs. Novell's Business Continuity Clustering (BCC) product offers a true cluster-of-clusters solution leveraging Novell's eDirectory service for cluster resource replication and management. BCC offers either manual or automated failover control between sites. Novell recently released an update that supports SUSE Linux servers; broadening application and service support greatly beyond simply NetWare file, print, and GroupWise services. Microsoft plans to include additional tuning parameters in Microsoft Cluster Services that are bundled in their planned release of Windows Server code-named “Longhorn” in late 2007 or early 2008. These tuning parameters will allow nodes to be grouped into tuning domains such that nodes local to one site may run with parameters that are different from the parameters controlling the groups across the stretch cluster, thus creating a quasi cluster-of-clusters.

Cluster-of-clusters approaches are recommended for geo-site solutions where distances greater than 100 km are deployed. Stretch clusters, while currently popular for shorter distances, should be upgraded and replaced with cluster-of-clusters solutions over time to improve reliability, allow for greater distances between sites, and reduce costs.

Geo-Site

For systems that do not require a strict RPO of zero (transactional data loss is acceptable),asynchronous replication is preferred.Synchronous replication or mirroring is required when a strict RPO of zero is required. Each has advantages and disadvantages:

Synchronous replication:

- **Pro:**
  - RPO = zero, no transactions loss for completed transactions
- **Cons:**
  - Application performance impacted by latency of link
  - Greater link costs to support higher bandwidth needs
  - Replication distance restricted to less than 100 km
  - More difficult to tune

Asynchronous replication:

- **Pros:**
  - Applications perform at local storage system speeds most of the time leading to better application performance
  - Lower link costs as bandwidth requirements can be lower
  - Replication distance is unlimited—may go halfway around the earth
  - Easier to tune
- **Cons:**
  - RPO > zero, completed transactions are lost
  - Heavy transaction loads over long periods of time which outpace the bandwidth of the data link may throttle application performance

Both synchronization methods require that the bandwidth of the site-to-site replication link be greater than the transactional data rate generated by the system over time. If the link bandwidth is less than the data rate generated over time, data will be lost regardless of replication method used.

Asynchronous replication results in lost transactions. As a result, application synchronization points are required to enable recovery at consistent transaction points. Snapshots achieve application synchronization points.CDP technologies may provide for finer-grained RPO by allowing a systems administrator to dial in specific transaction points newer than the latest snapshot in the recovery data. While this capability seems enticing, the use of CDP with asynchronous replication for DR is not worth the additional cost in storage required. (About 2.5 to 3 times more storage is required, depending on the size of the desired recovery window, which is typically from two to seven days.) Rather CDP is better suited for individual file or object restores, data audits, system development, and testing, all of which fall outside the scope of DR.

The most cost-effective solution for business continuity consists of snapshot checkpoints coupled with asynchronous replication. This combination reduces storage overhead and provides consistent RPOs by virtue of the application transaction points in the snapshots.

While it is the most costly solution, synchronous replication coupled with CDP offers fine-grained transactional recovery. While synchronous replication guarantees that completed transactions are not lost, transactions that were in process and not completed at the time of system failure may be recovered to some extent using CDP. CDP allows administrators to move backward one data block at a time from the point of failure until a consistent data point is located, which may be later in time than the last application consistency point. The *Data Center Strategies* overview, "Network Storage Virtualization: Technology Overview," explores CDP in greater detail.

Market Impact

Dramatic changes to the business landscape ushered in by e-commerce and the global economic reach afforded by the Internet have shaped new requirements in the twenty-first century for DR planning and business continuity needs.

Historical Market Needs

Prior to the e-commerce age, rapid DR and business continuity requirements for general-purpose and open systems existed mainly in the financial industry. Financial institutions are required to demonstrate disaster resilience in order to obtain Federal Deposit Insurance Corporation (FDIC) coverage and meet additional federal requirements. Other industries enjoyed small data sets and RTOs in hours or days. Traditional tape backup/restore easily met these needs.

During this era, both IBM and SunGard built DR businesses focused on serving the financial industry. SunGard built and maintains its own fiber-communications network between its data centers worldwide to meet these needs. Both IBM Global Services and SunGard continue to offer additional services to the financial industry, including software and financial processing systems.

The Internet and e-commerce era of the past decade brought financial industry-like requirements to many other industries. DR planning businesses sprang up to meet these needs. IBM Global Services and SunGard both expanded their businesses and offerings in the realm of DR planning and business continuity to meet the needs of e-commerce and digital media growth for industries beyond the financial industry. Improvements in manufacturing, e-commerce, digital imaging in health care, electronic B2B relationships, and many other systems have been automated via software, computer hardware, and networked devices. Manufacturing, retail, healthcare, government, and education sectors saw uptime requirements move from 8:00 a.m. to 5:00 p.m. Monday through Friday to 24/7.

Current Market Needs

The new e-commerce pressures of the twenty-first century have created new requirements in DR planning and procedures for virtually all businesses. These new requirements are:

- **Improve DR time** in order to meet the demands of the global economy. E-commerce availability requires service restoration within minutes of an outage to prevent financial disaster.

- **Reduce costs** for disaster recovery and disaster avoidance. Innovative technological advancements are able to both improve recovery speed and avoid disasters altogether.
- **Meet regulatory requirements** to avoid legal prosecution of executive staff and payments of large fines.
- **Minimize business downtime** to within minutes for e-commerce processes. Even maintenance downtime cannot be tolerated for critical systems.
- **Certify business processes** to avoid disasters as well as ensure rapid recovery should disaster strike. Just like ISO 9001-certified manufacturing processes are becoming requirements for business interaction, ISO 27001 data security certification requirements are beginning to grow.

Technology improvements are paving the way to meet these requirements:

- **Internet enabling technology shifts:** Internet bandwidth increases, broader availability, lower costs, and decreased latency have all improved business continuity for e-commerce.
- **Vendor technology improvements:** Sophisticated Internet-based replication and mirroring technologies, maturity in geo-site business continuity solutions, virtual machine technologies, D2D data protection, remote management tools, and competition driving down costs has placed business continuity and rapid recovery within the reach of more businesses, especially small to medium enterprises.
- **Co-location and hosting provider improvements:** Rapid growth in the number of co-location providers worldwide has led to increased competition and ubiquitous solutions. In addition to IBM and SunGard, multiple global, national, regional, and local co-location and hosting providers are now available. Many co-location and hosting providers now offer robust DR and business continuity solutions and services.

Market Impact by Industry

DR in each industry segment has generally seen increased need for lower RTO and RPO metrics while covering a greater number of systems. Most dramatic change in recent years has been in collaboration systems. E-mail has become a critical business system, requiring business continuity, with RPOs of near zero and RTOs in minutes or less. Requirements vary by industry. Furthermore, individual organizations within an industry will each have unique DR requirements. While each organization must perform detailed BIA on its individual systems, the following sections outline at a high level the general DR issues facing each market segment.

Financial

The financial sector continues to have the highest system value. Most financial brokerages indicate that one minute of downtime for one stockbroker equates to approximately $2 million in lost revenues. For this reason, the financial industry has the longest history of rapid DR and business continuity solutions.

While DR is mature in the financial industry, competition has unleashed a new bull in the market—cost reduction combined with extremely high data value and new regulatory requirements. Financial organizations are working to reduce both capital and labor expenses while maintaining and improving their business continuity solutions.

Health Care

Health care has recently seen two trends: Explosive growth in storage requirements fueled by digital imaging of medical X-rays, magnetic resonance images (MRIs), and other patient diagnostics records. HIPAA requirements have further exacerbated data growth, requiring patient records to be electronically secured, retained, and available. RPO and RTO metrics are required to be near zero for systems under HIPAA. Health care's current challenge is managing DR of explosive data growth resulting from digital imaging.

Government

Government systems are moving online to service citizens. Online transactions such as automobile registration and drivers license renewals are beginning to require 24/7 uptime from government IT systems. 911 emergency call centers and dispatch systems also require near zero RPO and RTO. Governments' challenges include handling increased data-retention requirements for DR.

Manufacturing/Services

Manufacturing and services have seen rapid growth in Internet e-commerce. B2B relationships with suppliers and distributors have demanded much lower RPO and RTO times than historically required. The manufacturing and service sector is struggling with ensuring improved DR of systems affected by increased data retention, and e-discovery requirements resulting from recent regulatory legislation such as SOX and FRCP.

Retail

Internet e-commerce has forever changed the retail business model. Customer business transactions via the Internet just scratch the surface. B2B electronic transactions to achieve lower stock-on-hand inventories through just-in-time supplier/distributor relationships are now common business practice. Competition has forced retailers into B2B relationships that mimic the Wal-Mart business model—squeezing every drop of overhead out of the product distribution stream. Retailers are struggling with extreme competition to reduce costs and overhead while meeting increased DR needs required by competition and new regulatory requirements.

Education

Education has moved many class and student registration systems online. Kindergarten through twelfth grade school systems are now working to meet the requirements of the No Child Left Behind Act. This act includes provisions giving parents secure and constant vigilance over their children's progress at school so that information such as grades and assignments is viewable online. Uptime, retention, and recovery requirements have forced educational institutions into a new realm of DR planning. Education is on the cusp of increased online courseware delivered via digital multimedia. As online courseware becomes a primary product, DR and availability requirements are being stretched to ensure that this new education business is protected.

Vendor Crystal Ball

Organizations embarking on DR planning may seek out consultants or other resources to assist in training employees for the planning and implementation process. Under no circumstances should DR planning be completely outsourced to a third party, as control of the DR process must remain within the executives' hands. Consultants can be used to design and implement systems, and train employees, but operation must be turned over to the permanent IT organization (which could include contracted, managed IT services).

DR planning, training, and system design comes from many different vendor angles. While larger consulting organizations offer DR services, many applications and infrastructure vendors offer consulting and best practices for DR designs specific to their products.

Large consulting vendors such as IBM and SunGard offer the broadest scope in DR system design and implementation. However, their experience is rooted in the financial markets, which may result in solutions that are more costly and over-architected for markets outside of finance. Furthermore, they may not have specific expertise on applications and systems that are not common in the market.

Medium-size consulting firms, while willing to accept most any DR or business continuity consulting opportunity, tend to focus in a particular area of strength. Electronic Data Systems (EDS), for example, tends to focus more on DR design for the healthcare market.

Most DR consulting firms are small and specialized to specific markets, applications, and systems. IT organizations should seek out small DR consulting firms for specific applications and services projects.

Preparing and training the employees of the organization in the principles of DR planning is of paramount importance to long-term success of a DR system. When an actual disaster strikes, the organization, not the consulting firm, must execute the plans. As a result, the employees must be completely trained and versed in the technologies used in the DR system.

Technology vendors continue to offer new and improved products and solutions for DR and business continuity. Generally, technology improvements are expected in these areas:

- Long distance data replication latencies caused by repeaters, switches and routing equipment will decrease through electronic improvements.
- Management tool improvements and new offerings in remote management and system deployment will improve speed and reduce costs in managing DR and business continuity solutions.
- Lower power systems, improved power conversion efficiency, and more efficient cooling systems will reduce the costs associated with alternate and co-located data centers.
- Virtual machine technologies will aid in driving down geo-site costs by enabling many-to-one business continuity failover scenarios. Virtualization can reduce capital expense, and utility and labor costs.

Consulting firms and technology vendors can offer knowledge and assistance in the DR planning process, but ultimately, the planning must be owned and executed by the organization.

Recommendations

Corporations must give heed to DR planning given that 25% currently have no or insufficient plans.[6] Lack of good DR planning indicates lack of fiduciary responsibility on behalf of the organization's executive staff. Organizations should utilize industry learning, consultants, and resources such as the ISO 17799:2005 requirements and ISO 27001 certifications to develop DR plans. Driven by executive staff, organizations should ensure continuous improvement by practicing DR plans, reviewing them often, and overhauling the plans when changes to business operations, regulatory requirements, or available technologies justify a change.

Geo-Sites

Pressures to compete and operate with reduced RTO and RPO metrics demand that more corporations than have previously done so invest in geo-site solutions. Organizations should analyze each system and associated data to evaluate its value to the corporation, and apply the corresponding DR or business continuity level to that system to protect against disaster. Involving partners and customers in the process must not be overlooked. Industry standard solutions for replication, including Internet Small Computer Systems Interface (iSCSI), should be used for site-to-site connections.

Burton Group recommends that businesses utilize the following approaches for recovery sites unless corporate policies, location, or cheaper existing premises dictate otherwise:

- **Cold site** should be contracted at the time of the disaster. Reservations should be minimal to no cost for such outsourced facilities.
- **Warm site** should not be considered. The costs outweigh the value.
- **Hot site** should be either a co-located or hosted facility.
- **Business continuity site** should be either a co-located or hosted facility if the corporation doesn't currently own a second data center located sufficiently distant from the primary data center.

Exceptions to these recommendations may occur. For example, a co-located or hosted recovery facility may be rejected if corporate policies dictate that data must be secured and controlled by the company and is not allowed to be outsourced. Additionally, co-location would not be an option if the required service area has an insufficient number of co-location providers.

Most large organizations already own alternate data center facilities. Such facilities, if located far enough from the main data center, may be utilized as a hot or business continuity site. Often, mergers and acquisitions between companies result in additional data center facilities. Corporations are advised, however, to analyze and compare the costs of continuing operations of an existing alternate facility with the costs of co-locating or hosting the services. Co-location may prove to be less expensive because of competition in the co-location market.

Data Protection

Traditional tape backup/restore should be relegated to satisfying long-term off-site archival and data retention needs. Tape is not dead, but continues to be the lowest-cost storage medium for large data sets (terabyte or larger systems) both in hardware costs and utility costs (electricity).

Burton Group recommends that customers consider replacing older tape backup systems with VTLs, D2D, replication, and snapshot solutions for those systems suffering from data growth. These solutions are able to keep pace with data growth and offer much improved RTOs. Furthermore, these solutions offer significantly improved restore times for individual file or object restore requirements. However, for DR, VTL systems should be replicated to alternate locations.

Co-Location

Organizations should consider co-location providers if not currently being used. Critical web- and Internet-based services are prime candidates for co-location. Non-Internet services, such as file and print, may not benefit from co-location or hosted services and should not be considered if the company already has alternate DR facilities. Corporations should leverage co-location provider competition to obtain the best price for SLA requirements.

Virtualization

Burton Group recommends that customers leverage virtual machine technologies to reduce costs and improved ease of DR and business continuity management. While most services can benefit from virtual machines, not all are suited to the technology. High input/output (I/O) throughput applications such as heavily loaded transactional databases will be hampered by virtualization and should remain on physical hardware. For all other services, virtual-machine management tools are required in order to achieve cost savings sufficient to justify the deployment.

The Details

Disaster recovery (DR) planning encompasses the entire organization, not simply the information technology (IT) services department. Preparing for contingent facilities and labor, building communication processes for employees, establishing plans with suppliers and distributors, and outlining actions to follow in order to quickly recover normal business operations are all required for successful recovery.

Planning for disaster avoidance should be done in addition to DR planning. For example, implementing proper information security controls and virus/spyware protection schemes helps to avoid potential security break-in or data loss disasters, or constructing facilities that can withstand tornadoes in “Tornado Alley.”

While DR planning is required for the whole organization, including all resources, functions, and facilities, the scope of this report is focused on IT systems and infrastructure: protecting the data center.

Disaster Planning Standards

The information security standard published by ISO 17799:2005 is a general, industry-agnostic standard that includes DR and business continuity planning (BCP). Most businesses that have implemented DR planning have utilized this standard. ISO 17799:2005 is a broad standard that is not specific to any particular vertical industry. The standard had its roots in the 1992 publication “A Code of Practice for Information Security Management,” which was created by Britain's Department of Trade and Industry. In 1995, the British Standards Institution republished it as BS7799. Then in late 2000, BS7799 was first published as International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17799. In 2005, ISO 17799 was updated to include two new sections. The update is called ISO 17799:2005. At that same time, ISO 27001 (which includes requirements for standard certification of ISO 17799:2005) was published. ISO 27001 provides for corporate standards certification for information security systems similar to that which the ISO 9001 certification standard provides for quality-management systems.

The ISO 17799:2005[7] standard contains 15 sections. Sections 1 to 3 include introductory notes, with the standards specifications beginning with Section 4. Table 1 provides a brief summary of the sections:

Section	Heading
4	“Information Security Risk Assessment and Treatment”
5	“Security Policy Management”
6	“Organization and Governance of Information Security”
7	“Information Asset Management”
8	“Human Resource Security Management”
9	“Physical and Environmental Security Management”

10	“Communications and Operations Management”
11	“Information Access Control Management”
12	“Information Systems Security Management”
13	“Information Security Incident Management”
14	“Business Continuity Management”
15	“Compliance Management”

Table 1: *ISO 17799:2005 Section Headings*

ISO 17799:2005 applies to more than DR and BCP. A number of subsections apply to disaster-avoidance planning. As primarily a security standard, implementing the standard in its entirety includes a level of disaster-avoidance planning for malicious security threats. The standard includes disaster-avoidance planning against other threats as well, including processes for identifying all threats that an organization may face. Section 14 applies to planning and processes that enable business continuity or immediate DR. Table 2 lists the sections applicable to disaster avoidance and rapid DR.

Section	**Description**
9.1.4	Protect facilities from natural or human threats
9.2.2	Reliability of supporting utilities
9.2.3	Secure power and telecommunications lines
9.2.4	Maintain data center equipment
9.2.5	Protect off-site equipment
10.1.1	Document operating procedures
10.1.2	Implement a change-control system
10.3.1	Capacity planning and usage monitoring

10.5.1	Back up your data and applications
10.7.1	Manage removable media
10.7.4	Protect system documentation
14.1.1	Establish business continuity for information
14.1.2	Identify events that could interrupt your business
14.1.3	Develop and implement your business continuity plans
14.1.4	Establish a BCP framework
14.1.5	Test and update your business continuity plans

Table 2: *Sections of ISO 17799:2005 Applicable to Disaster Avoidance*

As with any well-established process, ISO 17799:2005 follows the five basic steps generally accepted for project management: initiating, planning, executing, controlling and monitoring, and closing. This is especially evident in Section 14 for business continuity management.

ISO 17799:2005 Applicability to Disaster Avoidance

Selected sections other than Section 14 predominantly apply to disaster avoidance. They are described here to illustrate ways in which IT organizations can avoid local or smaller-scale disasters or events. Most of these are fairly obvious, but a surprising number of companies have failed to implement or maintain these standards.

The following is a simplified summary of those sections that are applicable to disaster avoidance.

9.1.4 Protecting Facilities from Natural or Human Threats

If a business's data center is located in an area prone to natural disasters, the data center should be resilient to those disaster events. Data centers located near California's San Andreas Fault should be built to withstand earthquakes. Data centers in the Southeastern and Midwestern United States should be hurricane and tornado resilient. While these measures will not protect from widespread devastation such as Hurricane Katrina, they can protect against smaller-scale disasters or attacks.

9.2.2 Reliability of Supporting Utilities

Generator backup for electrical power coupled with uninterruptible power supply (UPS) systems as well as multiple communications lines (telephone and data) also protect from local or smaller-scale disasters. Surprisingly, many disasters of this type are the result of human mistakes, such as a backhoe accidentally cutting through buried power lines or communications lines. Having redundant communication lines entering through a shared conduit is not a wise practice. Multiple communications providers further improve resilience from disasters.

9.2.3 Secure Power and Telecommunications Lines

Protecting the facilities entry locations of the electrical power and telecommunications lines helps avoid both natural and malicious disasters. For example, ice storms can break overhead power or communications lines.

9.2.4 Maintain Data Center Equipment

Fans, power supplies, disk drives, and any other mechanical equipment will wear out over time and require maintenance/replacement at scheduled intervals. Maintaining all equipment is simply preventative maintenance to protect against local outages of service, which could escalate into a disaster for business operations if not properly controlled.

9.2.5 Protect Off-Site Equipment

Off-site equipment contributes to the overall business operation, and must also be protected from natural or malicious damage. Off-site equipment in the context of IT services applies to co-located or alternate data centers.

10.1.1 Document Operating Procedures

In the case of disasters that prevent the workforce from coming to work or worse, injure or take human life, alternate resources must be employed to keep systems running. Without documentation, operations may not be able to continue, or may be severely hampered resulting in service and business disruption.

10.1.2 Implement a Change Control System

Change control is necessary to ensure that operating procedures and system configurations are properly updated. Alternate sites and redundant systems are also included in any operational update or change. Without change control, the alternate, backup, or redundant systems and data called on for DR will be improperly configured and result in further delay, even the possibility that operations cannot be restored.

10.3.1 Capacity Planning and Usage Monitoring

Lack of capacity planning based on usage monitoring can result in a systems failure and business interruption due to insufficient storage or insufficient peak compute capacity. Usage monitoring should be done throughout the year in order to understand the dynamics of the organization. For example, an accounting firm's IT group may find nominal storage growth during most of the year, but miss accelerated storage growth a few weeks prior to 15 April (U.S. income tax due date).

10.5.1 Back Up Your Data and Applications

Copies of data and applications as well as associated system configurations provide the best protection. The copies should be physically separate from the facilities to ensure they are not destroyed in a widespread disaster. If one copy is good, two copies are better if they are in separate locations. Many methods exist for backing up data, applications and associated system configurations. The *Security and Risk Management Strategies* overview, "Backup and Recovery," delves into backup and recovery techniques from the perspective of data risk management.

10.7.1 Manage Removable Media

Removable media (such as tape archives) must be under policy management control, and must be tracked and regularly tested to ensure recoverability. If required for DR, removable media should be quickly locatable and usable.

10.7.4 Protect System Documentation

Along the lines of Sections10.1.1 and10.1.2, the operating procedures and system configuration information must also be protected. Copies should be placed in secure but known locations such that they can be retrieved in the event of a disaster. More than one individual should know where these locations are and how to access them. If possible, geographically separate sites or even a third-party site such as a safe deposit box should be used. Printed and electronic copies of the system operations documentation should be placed in the safe deposit box or other secure remote location.

ISO 17799:2005 Applicability to DR

Section 14 of ISO 17799:2005 applies to business continuity or rapid DR. This section forms the heart of the standard's focus on disaster planning. Prior to the 2005 update, this was located in Section 11 of the earlier ISO 17799 standard. The *Security and Risk Management Strategies* overview, "Business Continuity Planning for IT," analyzes Section 11 of the original standard in detail. The overview recommends the ISO 17799 standard and describes the strengths and weaknesses of implementing Section 11 of the standard. The overview only covers Section 11 of the original standard.

14.1.1 Establish Business Continuity for Information

Section 14 of ISO 17799:2005 contains elements for initiating BCP. This section is the primary basis used for developing DR plans.

14.1.2 Identify Events That Could Interrupt Your Business

Identifying the possible events that could interrupt a company's business is a first and critical step to preparing and implementing a plan. The *Security and Risk Management Strategies* overview, "Business Continuity Planning for IT," points out that the standard is weak in this area. The standard only identifies events and lacks guidance on identifying sequences of events or complex event scenarios. In real world disasters, event sequences are what actually occur. Businesses must understand the more complex relationships and consequences of event sequences in order to successfully prepare for DR. In addition, businesses should prioritize possible events. For example, in "tornado alley" the possibility of power outage is much greater than a direct tornado hit on the facilities.

14.1.3 Develop and Implement Your Business Continuity Plans

This section outlines the process of implementing business continuity plans. Included are the requirements to identify the procedures that individuals and groups will follow in the event of a disaster. This planning includes the external contacts, supplier and distributor relationships, and how they will be managed. Budgets for ongoing plan management and testing are also identified and allocated.

14.1.4 Establish a BCP Framework

The framework is the actual plan, which includes identifying the triggers that will invoke the plan and indicating who will carry out the plan. Contingencies are also outlined in case primary individuals or groups responsible for executing the plan are not available. The framework also includes the termination of the plan execution at the conclusion of a disaster event. Typically, the executive staff will declare the disaster and invoke the disaster plan. A chain of command exists to invoke the disaster plan in case the executive staff is not available when a disaster strikes.

14.1.5 Test and Update Your Business Continuity Plans

Ongoing quality assessment of the plan is required. The infrastructure to review and update the plan to match organization and operational changes that occur over time is included. Regular testing of the plan is specified, with specific training, especially for new employees or in the event of other organizational changes.

Aside from ISO 17799:2005, a few vertical industry-specific standards and standardization efforts exist. These are not general, but apply to specific markets and segments. Corporations should follow DR guidelines and regulations that apply to their specific market segment in order to augment planning from the ISO 17799:2005 standard. Examples of industry vertical standards are the Financial Services Technology Consortium (FSTC) and Federal Emergency Management Agency (FEMA) disaster recovery planning standards.

Technologies for DR

Numerous technologies exist to aid in IT systems DR. In recent years, the options and techniques have been changing as the result of moving requirements being placed on system administrators as well as technological advances coming from vendors. The following technologies have either improved over time or are new inventions/concepts in the market that target DR. The new inventions specifically target rapid DR or business continuity.

At the highest level, the principles of data and system recovery include multiple copies of data, configurations, and systems. The following technologies are all about copies and system redundancy.

Removable Media Technologies

Removable media includes any media that is easily removed for transport or storage at a different location. This includes tape, removable disks, and removable flash RAM. In this section, only removable media that is typically used for backup and archival purposes will be discussed. Floppy disks, universal serial bus (USB) flash or jump drives, and hot swap hard disks will not be discussed, as they typically are not considered archival media. CD jukeboxes are also not discussed, as they are considered static data resources (guides and manuals).

Magnetic Tape

Magnetic tape drives represent the oldest and the most mature removable media technology on the market for making copies of data, which may be easily transported. The most popular formats in recent years have been Digital Linear Tape and Linear Tape-Open. Multiple manufacturers employ both formats (although Digital Linear Tape is manufactured under license from Quantum).

Magnetic tape is written and read in a sequential fashion. Tape is not designed for random access. This makes magnetic tape best suited for streaming large amounts of data, such as a whole server volume backup or restore. Tape is not well suited to individual file lookup, searching, or indexing which processes require random access.

Densities and speeds of magnetic tape drives have increased over the past two decades. Additional technological advances have been made in tape drive mechanics, electronics, and firmware to increase density, speed and reliability.

While most manufacturers will list device speeds and capacities assuming a 2:1 compression ratio of the data, this does not represent real live modern data, which typically may only achieve a maximum compression ratio of 1.5:1.

Manufacturers guarantee a 30-year data retention life of modern magnetic tape media when stored under specific environmental conditions.

Manufacturers typically guarantee that modern drives can read older tapes that were written using two-generation prior technology. They also typically guarantee that modern drives can write to one-generation prior technology tapes.

Digital Linear Tape

Digital Linear Tape (DLT) has its roots in technology developed by Digital Equipment Corporation (DEC) back in 1984. Ten years later, Quantum purchased the technology and continued innovating to increase speed and capacity of DLT. Quantum changed the name in 1998 on the introduction of much higher capacity drives and media to Super DLT, or SDLT. More recently, the name was again changed to DLT-S4.

Table 3 outlines the recent technological advances of SDLT technology:

Year	1998	2002	2004	2006
Product name	SDLT 220	SDLT 320	SDLT 600	DLT-S4
Native speed (MB/s)	10	16	36	60
Native capacity (GB)	110	160	300	800

Table 3: *Raw Speed and Capacity Improvements of SDLT*

Vendors: Quantum, Hewlett-Packard, IBM, and Dell.

Linear Tape-Open

Linear Tape-Open (LTO) is a more recent open standard that was developed as a collaborative effort among Seagate, Hewlett-Packard, and IBM. First released in 2000, LTO was developed as an open alternative to DLT. The tape cartridges and drives are close enough in size to their DLT counterparts such that either technology can be interchanged in robotic systems such as large automated tape libraries. Table 4 outlines the technological advances over time of LTO technology.

Year	**2000**	**2002**	**2005**	**2007**
Product name	LTO-1	LTO-2	LTO-3	LTO-4
Native speed (MB/s)	20	40	80	120
Native capacity (GB)	100	200	400	800

Table 4: *Raw Speed and Capacity Improvements of LTO*

LTO includes a variable-speed feature. This feature allows the drive to slow down in order to pace data transfer if the host is unable to provide data at the tape drive's maximum capable rate. LTO-3, for example, can vary its data-streaming speeds from about 30 MB/s to the full 80 MB/s.

Vendors: IBM, Hewlett-Packard, Quantum, Tandberg Data, and Dell.

Tape Auto-Loaders and Libraries

Tape auto-loaders and libraries combine mechanical robotics, tape drives, and tape cartridge storage shelves into a single unit. Typically, auto-loaders are small with only one drive and limited tape cartridge storage. Libraries can be massive, containing several tape drives and up to thousands of tape cartridges for total storage capacities in the petabyte range (1,024 gigabytes).

Large tape libraries offer the most economical method of storing massive amounts of data, but because of the time needed to retrieve and load a cartridge into an available drive, the performance suffers greatly for random access patterns. Based on tape drive technology, libraries only offer sequential read/write of data from and to the tapes. Larger libraries present great economies of scale, achieving costs per gigabyte of around only 10 cents.

For off-site storage, tape libraries typically have a slot or mailbox by which tape cartridges may be accessed for movement to off-site facilities. The software managing the tape library will present the cartridges through this slot to the operator for removal and shipping off site based on policy configured in the system.

Vendors: StorageTek (Sun Microsystems), ADIC (Quantum), Overland Storage, Spectra Logic, Tandberg Data (Exabyte), IBM, Hewlett-Packard, Dell, M5 Data, Qualstar, and Rorke Data.

Removable Disks

Removable disks were developed after tape with the intent of offering long lasting archival properties that are simpler to use and more resistant to abuse. Recordable CD, DVD, and magneto-optical (MO) devices are used for long-term archive. Removable hard disks, such as those produced by Iomega a number of years ago, are no longer used nor produced as they suffered reliability and lifespan problems.

Long-term archive technologies are not within the scope of this report. Suffice it to say that long-term archives are useful in recovery of noncritical systems and data.

Backup/Restore Software

Backup/restore software for removable media has been available for more than three decades. In its simplest form, backup/restore software programs, manage the copying of data on fixed media devices (server hard disk) to and from removable media such as tapes.

Current backup/restore software includes sophisticated features to enable complete restore of data, systems, and configurations. DR scenarios require not only restoration of the data, but also the operating systems, applications, and their associated configurations.

Backup to tape methodologies fall into three general categories:

- **Full backup** includes a complete copy of all the files on the server volume that is being protected.
- **Incrementalbackups** are done following a full backup. Incremental backups only copy the files that have changed since the previous incremental or full backup. The complete restore set using this method includes the full backup and all incremental backups taken since the full backup.
- **Differentialbackups** improve on incremental backups in that each differential backup includes all the files that have changed since the last full backup and not the previous differential backup. The complete restore set using this method includes the full backup and the most recent differential backup. A complete system restore is faster using differential backups than it is with incremental backups because finding and mounting various incremental tapes takes longer, but the size of the differential backup sets is larger.

Recent advances in backup/restore software include additional features that are more suited to DR. These include, but are not limited to:

- **Snapshot backup:** A snapshot of the server's volume is made and then the snapshot of the volume is backed up. This feature allows a consistent view of the volume from a single point in time, without disrupting the ongoing operations of the server and its applications. Applications integrated with snapshot frameworks, such as Microsoft Windows Server 2003 Volume Shadow Copy Service (VSS) are informed that a snapshot is going to take place and are given to opportunity to flush data to disk to ensure that the snapshot taken contains a consistent and up-to-date view of the application's data.
- **Image backup:** Enables a backup/restore of not only the data, but also of the operating system, applications, and configuration. This is accomplished by copying an image of the system volume and application volumes. While image backup solutions have existed for some time, virtual machine backup/restore has made more recent use of image backup because of the increased ease of obtaining, deploying, and managing virtual machine images as compared with physical machine image backup/restore.
- **Application-specific backup agents:** Allow the backup/restore software to work directly with the application instead of the file system. A backup/restore program working with a file system that contains Microsoft Exchange files would not understand the relationship between those files. The backup program would not know which file sets make up a particular user's mailbox, for example. But by working through a Microsoft Exchange-specific backup agent, the backup/restore program would be able to backup and restore the data in the context of its internal relationships. The backup/restore program in this case would know which files or messages were associated with a particular user's mailbox, and so forth. The Exchange backup agent interfaces with application programming interfaces (APIs) exported by Exchange as opposed to interfacing with the file system. Similar agents are typically available for common applications and databases in the industry.
- **Continuous data protection (CDP):** Makes a copy of the data as data is written. Traditional backup/restore systems are batch process-oriented. CDP is continuous data flow-oriented. Details onCDP are discussed later in this report.

Vendors: Symantec (Veritas), IBM, EMC, Hewlett-Packard, CommVault Systems, CA, Syncsort, BakBone Software, and Yosemite Technologies.

Storage Technologies

Historically, fixed-disk technologies, which not only include hard disks, but also any storage that is typically not removed to archive, have been the preferred storage medium for active data. This trend continues to date, even in light of research into silicon-based storage or other forms of active storage, because of the simple economics of the storage medium.

Hard Disk Drives

Hard disk drives (HDDs) continue to drop in price and increase in capacity following a trend similar to Moore's Law (Moore's Law applies to computer processor transistor density increases). HDD capacities have increased at an exponential rate over the past two decades. Table 5 illustrates this point, with capacities of Industry Standard Architecture server and desktop hard disks (5.25″, 3.5″) increasing at a rate of about tenfold every five years:

Year	**1987**	**1992**	**1997**	**2002**	**2007**
Disk capacity (GB)	0.1	1	10	100	1,000

Table 5: *Capacity Improvements of HDDs*

While the capacity of HDDs has increased exponentially, performance factors have not increased at the same pace. Three factors dictate performance of HDDs: disk rotational velocity (how fast the platters spin), aerial density (the amount of data packed into one square inch of platter surface), and access times (how quickly the read/write heads can position themselves to the proper track and sector on that track to begin reading or writing data).

Access times have not improved as much as have capacity increases and data throughput. Access times have only improved threefold in 10 years. Data throughput has increased about twentyfold in 10 years. However, disk buss technologies limit the actual throughput in many cases and these maximum improvements only figure for sequential disk reads in which access time is not a gating factor.

Disk performance and capacity improvement summary over a 10-year period:

- **Capacity:** 100 times
- **Throughput:** 20 times
- **Average seek time:** 3 times

Data Replication

Data replication technologies include software and hardware products that copy and synchronize data from one fixed-storage device to another over a storage area network (SAN), local area network (LAN), or wide area network (WAN) medium. Replication can be done at the block storage level (at the disk drive or storage array), or at the file or application level (at the file system or application interface). Application-level replication must be accomplished at the host. Data replication is further subdivided into synchronous and asynchronous replication.

Block Replication

Computer storage systems typically read and write data in blocks of a given size. HDDs store and retrieve data in 512 byte sectors. The protocols for reading and writing block-level devices are rather simplistic. A given block address is specified for reading or writing on a given device. For efficiency, standard file systems typically will read and write data in larger chunks. 4,096 bytes (4 KB) is the most common block size.

Block replication solutions as a result of the simplicity of the interfaces, do not need to know anything about the data structure on the device. They only need to know the device physical parameters, such as the storage device's size. For efficiency, block replication solutions will also copy data in larger chunks than a physical device sector size. Industry standard (x86) server operating systems utilize memory page allocation sizes of 4,096 bytes. Therefore, replication software using this size, or multiples of it, will gain efficiencies from the system.

Storage virtualization solutions, such as volume managers, maintain the same interfaces and parameters as physical devices allowing block replication solutions to operate equally well with virtualized logical devices and physical devices.

File and Application Replication

File-based replication solutions operate only with the host file system or specific applications running on the host server. Application-specific replication solutions interface with the application they support. Examples of application-specific replication solutions are Oracle's basic and Advanced Replication.

Much more information about the data is available from the file system or application interface level. Metadata, such as file name, size, type, creation, and modification, is available at the file-system level. Application-specific replication solutions gain additional semantic information about the data, such as database table structures and relationships. The additional metadata available allows file and application replication solutions to filter content and apply replication policy based on content (such as selectively not replicating music files).

Synchronous Replication

Synchronous replication, or mirroring, ensures that the data is written to both the primary storage device and the secondary storage device in unison (see Figure 5). The host applications or services writing the data are not allowed to continue to the next operation until both copies of the data have been successfully written. Exact copies of data at the primary device and the secondary device are ensured at all times by virtue of synchronous replication.

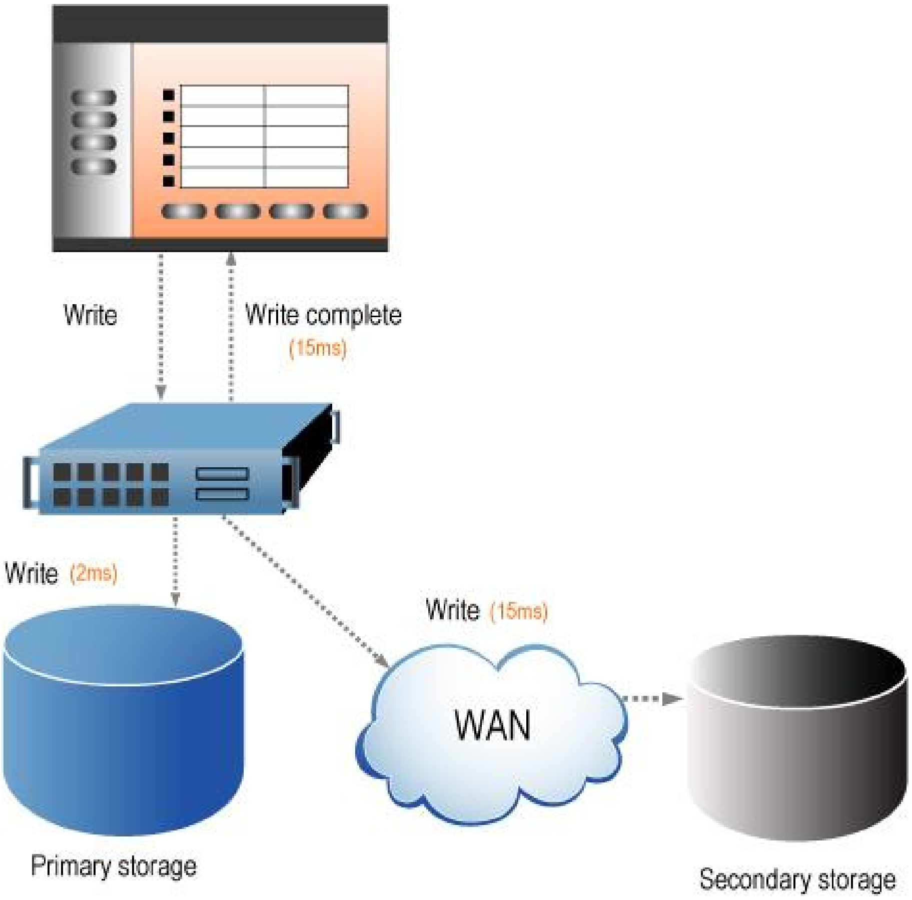

Figure 5: *Synchronous Replication (Mirroring)*

Communication latency in the WAN link not only throttles application performance, but also restricts the distance over which synchronous mirroring may be accomplished. Typically this is limited to 100 km or less.

Asynchronous Replication

Asynchronous replication copies previously written data on the primary storage device to a secondary storage device. Asynchronous replication does not force the host services or applications to wait until the data is written to the secondary storage device before these applications move to the next operation (see Figure 6). The drawback to this approach is that the data is not kept in strict synchronization between the primary and secondary storage devices. The secondary is always some time behind the primary.

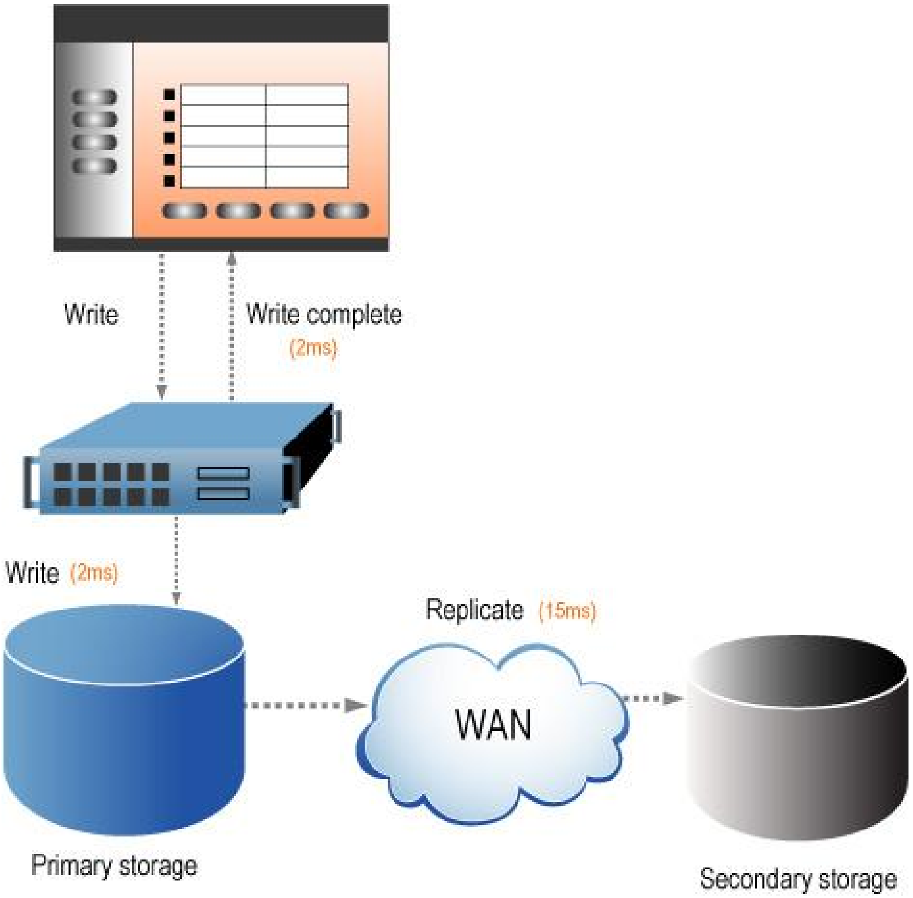

Figure 6: *Asynchronous Replication*

Two methods exist in the industry for accomplishing asynchronous replication:

- **Buffered replication** utilizes a memory or disk buffer to immediately store the data to be replicated just prior to replication. The memory buffer allows the system to absorb spikes in data throughput without sacrificing application or service performance. However, if the buffer becomes full because the replication link cannot keep up, the host applications and services are throttled until the replication to the secondary storage device can catch up. If the replication link connectivity is lost, the replication ceases, allowing the applications to continue. Many vendors classify buffered replication as synchronous or semi-synchronous replication. However, because the data between both primary and secondary devices is not in strict synchronization all the time this method is asynchronous.
- **Snapshot/copy replication** combines storage snapshot with a copy solution. A snapshot of the primary storage is made, followed by copying of that snapshot image to the remote secondary storage. Many vendors include efficiencies to only replicate the changes between snapshots, which greatly reduces the link bandwidth required. Advances across all operating system environments in recent years include application integration with the snapshot technology so that the application is informed that a snapshot event is about to occur. The snapshot event allows the application to flush its data buffers and ensure that its data in the primary storage is in a consistent state just prior to the snapshot occurring. Microsoft's VSS includes such an infrastructure. Additional advances include snapshot copy logic, which can recognize and move only those data blocks that have changed since the previous snapshot, thereby significantly lowering the bandwidth needs of the data link between the primary and secondary storage.

Vendors: BakBone (Constant Data), CA (XOsoft), DataCore Software, EMC (Kashya and Legato Systems), FalconStor Software, Fujitsu Software (Softek Storage Solutions), Hitachi Data Systems, Hewlett-Packard, IBM, LSI Logic, Network Appliance (NetApp), NSI Software, Radiant Data, RepliWeb, Sun (StorageTek), Symantec (Veritas), and a number of other smaller vendors and open source solutions (such as DRBD and rsync).

Where's the Replication Engine?

Data replication solutions can be implemented in one of three locations in a storage system: the host server, the storage network, or the storage array. Replication solutions implemented at the storage network or storage array are specific to the type of storage network: SAN or network-attached storage (NAS). Table 6 indicates network type, level, and replication type.

Replication solution	**Host**	**NAS network**	**SAN network**	**NAS array**	**SAN array**
Block based	**X**		**X**		**X**
File based	**X**	**X**		**X**	
Application based	**X**				

Table 6: *Replication Engine Location in the Storage Stack*

Restoring Replicated Data: Promotion to Primary

Synchronous and asynchronous replication solutions copy data from a primary storage device to a secondary storage device. However, servers attached to secondary storage devices cannot access the replicated data until those storage devices are promoted from secondary to primary. Masking servers from secondary devices prevents data corruption, which could be caused if servers and replication software attempted to simultaneously write to the secondary storage.

SANs and replication software work in concert to control the promotion of secondary storage devices to primary storage devices and the demotion of primary storage devices to secondary storage devices. When disaster takes out a primary site, automated or manual processes must promote the secondary storage to primary. At that same time, the replication software no longer writes to the storage, but has the option of copying from the newly promoted primary storage to a another secondary storage device.

SANs include APIs and scripting interfaces to control storage device promotion and demotion. Business continuity solutions leverage these interfaces to control site-to-site failover.

Disk-to-Disk Backup

Disk-to-disk (D2D) backup, sometimes backup to disk (B2D), comes in multiple flavors, all of which fundamentally make data copies to disk as opposed to tape. Software solutions provide for a myriad of features and capabilities when applied to D2D systems. Data replication, disk images, snapshots, CDP, and virtual tape libraries (VTLs) all leverage D2D backup.Data replication is the simplest example of D2D backup. Disk image copies create an image of a disk in a file, offering a different form of B2D. Snapshot technologies are implemented in one of two general forms: full-image snapshot and copy-on-write (COW) snapshot. Full-image snapshots produce a full data copy of the volume at a point in time. EMC uses the term "Business Continuance Volume" (BCV). Hewlett-Packard uses the term "Snapclone." NetApp uses the term "SnapMirror." In these cases, the whole snapshot data image is copied to new storage, whether inside or outside of the storage array. COW snapshots do not require a full copy of data, but maintain only the changes with references back to the original unchanged data. COW snapshots consume less storage, but depend on the original data. CDP adds a time dimension to D2D backup.CDP is discussed in the next section.

VTLs are a unique form of B2D. A VTL replaces a tape library with disk storage, while maintaining the tape library interfaces. This allows the use of existing backup software as well as IT backup/restore procedures. System operation does not require retraining IT personnel, or investing in new software.

Continuous Data Protection with Replication

Continuous data protection (CDP) solutions are similar to snapshot/copy with the added dimension of time. Most include a replication option to copy the data images to secondary storage. In CDP, each copy of the primary data is tagged with a time marker enabling a systems administrator to move to any previous point in time within the data image. This can be done in two ways:

- **Multiple snapshots** simply mark each incremental snapshot image with a time marker. The snapshot interval is configurable, usually down to one minute. Applications integrated with snapshot for consistent data images offer advantages to this approach. In addition, the amount of storage required for this method is much less than CDP journaling. The amount of additional storage required is dependent on the number of snapshots desired and the type of snapshot (full or COW).
- **CDP journaling** (or transaction-based CDP) marks each changed data block with a time marker. The advantages are that the data image can be rolled back to any instant in time. This fine-grained approach offers the advantage of rolling back to the instant just prior to a data corruption event. The disadvantage is that approximately 2.5 to 3 times additional storage is required to support this approach.

Storage consumption of CDP can be great. Administrators allocate storage to the CDP system, which must be larger than the data to be protected. The amount of additional storage dictates the recovery window (the amount of fine-grained CDP journal). As a rule of thumb, allocating three times the storage for the CDP journal will yield a one-week recovery window (your mileage may vary).

Vendors: Availl, EMC (Kashya), FalconStor, FilesX, Mendocino Software, NetApp (Alacritus Software and Topio), and Symantec (Revivio).

Server Technologies

Server operating systems have improved to take on the challenges of DR and business continuity. From operating system enhancements to built-in high availability clustering, modern x86-based operating systems now include the basic features necessary for business continuity.

Dynamic Hardware Discovery

Windows, Linux, NetWare, and Solaris (x86) operating system releases since around 2003 brought dynamic hardware discovery capabilities. Initially implemented to support blade server deployments, dynamic hardware discovery allows an operating system to automatically configure itself to new or changed hardware. This feature is important to DR because identical hardware may not be available at the recovery site. Differences in hardware adapters require associated device drivers. As such, dynamic hardware discovery can simplify and speed recovery operations.

High Availability Clustering

Customers have utilized high availability (HA) failover clustering solutions for a number of years to ensure service and application uptime. HA clusters bring two or more physical server machines with SAN attached storage into a cluster group. HA cluster software continuously monitors the health of each server and the applications/services running on the server. The HA system relies on the cluster heartbeat, a tightly coupled communications system, to relay health of the system between all server nodes in the cluster. Failures occurring on a server, whether an application, service, operating system, or the server hardware itself are detected and rapidly communicated resulting in the affected application or service automatically restarting on a surviving server node in the cluster. Administrator-determined policies dictate where applications and services will move in the event of a failure to avoid problems such as overloading or lack of resources. HA cluster solutions include application-dependency policies to ensure that when an application is restarted on a surviving cluster node all of the application's required resources, such as storage volumes, Transmission Control Protocol/Internet Protocol (TCP/IP) addresses, helper applications, and the like, are available to the application.

While HA clustering solutions have been utilized by corporations to protect against localized failures for some time now, more recently forward-thinking customers have been employing geo-site clusters. A variation on the HA cluster theme, geo-site clusters protect against wide-scale disasters.

Vendors: Hewlett-Packard (including PolyServe), IBM, Sun, Microsoft, Novell, Red Hat, SGI, SteelEye Technology, and Symantec (Veritas).

Geo-Site Clustering

HA cluster value propositions have recently been leveraged to a broader scale beyond the confines of a data center. Stretch clusters and cluster-of-clusters coupled with data replication solutions have been developed to enable automatic application restart on servers located in a distant location, safely away from a wide-scale disaster.

Stretch clusters split the HA cluster server nodes between two geographically separated data centers. Logically, the server nodes are all part of a single cluster with tightly coupled heartbeat communications between all the nodes, even across the distant link that connects the two data centers. While this configuration seems simple, issues can arise resulting from the physical distance between the two data centers.

Cluster-of-clusters lacks tightly coupled heartbeat communications between the two data centers, which alleviates the distance problems associated with stretch clusters.

Propagation delay affects the communications over a wide area link because the speed of light is a finite number: 300,000 km/second in a vacuum. The refractive index of the glass used in a fiber-optic cable reduces the speed of light to an effective speed of just over 200,000 km/second.[8] For simplicity of example, assume two sites are 500 km apart. Communications request and reply must travel in both directions, resulting in a roundtrip distance of 1,000 km. Communications propagation delay would be five milliseconds in this example. This is a theoretical best case, as a practical implementation would have some number of electronic repeaters, communications switches, and signal boosters along the 500 km path—all of which will interject further propagation delays. Modern fiber cables are capable of distances around 100 km between repeaters or signal boosters[9]. More importantly, stretch clusters typically cannot operate effectively over distances greater than 100 km because of latency impacts on their heartbeat communications between the sites.

Vendors: Hewlett-Packard, IBM, Sun, Microsoft, Novell, SGI, SteelEye, and Symantec (Veritas).

DR with Virtual Machines

Virtual machines have recently found their way in to providing unique and cost effective DR solutions. A number of characteristics of virtual machine technology enable and simplify DR processes.

First and foremost is the solution to the hardware version problem. Disasters many times involve destruction or loss of server hardware. Reinstalling an operating system on new hardware can be a time-consuming process and simply attempting to copy the operating system to alternate hardware often results in driver and configuration mismatches. Specific hardware versions may no longer be obtainable and configurations may clash. Restoring from an image also exhibits similar compatibility issues. Virtual machines, however, insulate the operating system from the physical hardware, as well as nicely separate the server-specific configuration from the operating system. The result is that a virtual server can be quickly provisioned without regard to drivers and server-specific configurations.

DR may not require all critical services to run at full production capacity initially. Recovering servers and services into virtual machines offers the added benefit of reduced standby hardware, mitigating overall investment and operating costs.

Recent management tools from VMware and other virtualization vendors include automated virtual machine resource management, which can be configured to automatically move virtual machines to servers located in separate locations. These tools are akin to HA cluster solutions except that they are specific to virtual machine resources as opposed to ensuring HA of specific applications or services.

Testing DR scenarios can be facilitated by virtue of virtual machine technologies, as deployment and termination of virtual servers can be accomplished using existing physical hardware.

As with any nascent technology, virtual machine applicability to data protection and DR is still rough around the edges. The *Data Center Strategies* report, "VM Backup Bliss? The State of VM Data Protection in the Enterprise ," exposes the land mines and pitfalls of virtual machine protection as well as exploring the values of the technology.

DR Providers

DR providers have offered services for nearly three decades. However, recently co-location data center providers have sprung into existence over the past decade to offer additional compelling DR and business continuity options.

Off-Site Tape Archive

Copies of data on magnetic tape, digital versatile disc-recordable (DVD-R) or MO media stored at the primary data center facility offer only localized DR. Disasters such as localized data corruption or loss from malware or human error can be recovered from these local backup copies. Additionally, loss of a physical machine due to hardware failure can be recovered locally. However, local storage of backup media does not protect from site-wide disasters.

Vendor-managed off-site backup media archive facilities offer three main features:

- The data is physically separated from the data center, for preservation in the event of a site-wide disaster.
- The off-site archive facilities are environmentally secure and controlled to ensure data longevity and safety.
- Media is tracked electronically so that retrieval is fast and accurate, and rotation and destruction policies can be properly applied.

Many backup media archiving facilities vendors offer DR planning and execution services. These services allow customers the ability to utilize the off-site vault for more than just backup media storage. Disaster plans may also be stored with the vendor, and the vendor acts as an independent contact point for the customer's employees to utilize during a disaster. The archiving facilities vendor may act as the emergency operations center (EOC) if necessary.

Large disasters that take out an entire data center require that a new data center be constructed and the off-site backup media be transported to the new data center facility. Otherwise a contracted or leased recovery facility can be employed to shorten recovery time. This is known as cold site recovery.

Data recovery is only up to the most recent media that was shipped to the facility, leading to only stale data available for recovery. A typical tape off-site transport policy of once a week may result in stale recovery data of up to one week old.

Vendors: IronMountain and various regional or local vendors.

Off-Site Data Vault Facility

Off-site data vaults improve on off-site tape archives in that the data is electronically replicated to disk storage systems at the off-site facility. Data is constantly kept up to date via replication for timely recovery. Stale data issues associated with tape archives are mitigated. Data is secured and encrypted, and can be further replicated by the provider to ensure additional protection (in case the provider loses a data center).

Recovery from a data vault is achieved either via Internet connection download or overnight shipping of NAS appliances based on customer preference and data amount. Available Internet bandwidth and data set size dictates which method is fastest for recovery. Larger data sets may be obtained quicker if shipped overnight on a NAS appliance.

As with off-site tape archive, cold site recovery with a contracted recovery facility may also be required to supply the server and network infrastructure needed to access the data.

Vendors: IBM, SunGard, and numerous regional and local Internet data vaulting providers such as U.S. Data Trust, Data Protection Services, Data Vault, Northeast Data Vault, AmeriVault, and more.

Off-Site Recovery Facility

Off-site recovery facilities offer full data center infrastructure and equipment to quickly reconstruct a customer's critical data center environment. Off-site facilities can either be permanent installations operated by DR providers, or mobile units built inside semi-tractor trailers, which can be transported into any location needed. Off-site recovery facilities differ from co-located or hosted facilities in that customer's data and applications are installed and operated at these facilities only in the event of DR.

Vendors: IBM and SunGard.

Co-Located and Hosted Data Centers

Leasing Internet connected data center server rack space to customers gave birth to the co-Located data center business model. The growth of e-commerce has increased customers' data center appetite for Internet bandwidth. These burgeoning Internet bandwidth needs subsequently created the opportunity for vendors to supply customers with rentable data center space outfitted with direct connections to high-bandwidth Internet providers. Corporations have benefited from both increased Internet bandwidth and lower Internet connectivity costs at co-located data centers.

The co-location model inherently benefits from the savings associated with economies of scale. Internet service providers and Internet consumers both benefit by locating their equipment in the same physical premises. Co-location centers offer state-of-the-art data center facilities including redundant high-speed Internet from multiple carriers, diesel generator power backup, redundant geographically separated data centers, and surveillance/security systems. Multiple customers share these costs resulting in lower individual company expense as opposed to owning and maintaining their personal data center.

Hosted data centers have sprung up as a thriving and growing business. The origins of this business have their roots in the dotcom growth era, as corporations rushed to gain a web presence for their products and services. Those early web server farms required high-bandwidth Internet access, which was not readily accessible to older data centers. So entrepreneurs would lease rack space from co-location providers, outfit them with web servers, and sell the web content creation and management to customers. From their website hosting origins, the hosting business has branched out offering virtually all traditional data center operations and management as a remotely located consumable service. Furthermore, application service providers (ASPs) have sprung into business, offering Internet hosted application services to customers.

Vendors: Numerous worldwide, regional, and local co-located and hosted data center providers such as AT&T, Cervalis, Connectria, ColoSpace, Data Foundry, Data Return, IBM, Nacio Systems, NaviSite, Northeast Data Vault, Qwest Communications, Rackspace, Savvis, SunGard, US Internet, VeriCenter, Verizon, and more.

Conclusion

Business and market changes of the new global economy coupled with the explosion of digital media have made obsolete the traditional methods of tape backup/restore for corporate disaster recovery (DR). Advances in business continuity technologies, heavier reliance on information technology (IT) systems to meet competitive e-commerce needs, and regulatory legislation are forcing top executives to reformulate their DR solutions. DR planning is not insurmountable, however. Organizations can utilize new standards, methodologies, services, and technologies to create viable DR and business continuity solutions at marginal cost.

Notes

[1] Darrell Dunn. “Many Data Center Still Have No Risk Management Plan.” *InformationWeek*. 21 Mar 2006. http://www.informationweek.com/showArticle.jhtml;jsessionid=SFFMOHOUSGUJUQSNDLRSKHSCJUNN2JVN?articleID= 183701425&queryText=data+center.

[2] Allan Sloan. “Skies Were Cloudy Before Jet Blew It.” *MSNBC: Newsweek*. 5 Mar 2007. http://www.msnbc.msn.com/id/17313450/site/newsweek/.

[3] “Natural Disasters on the Rise.” *Washington ProFile*. 28 Apr 2005. http://www.washprofile.org/en/node/3381.

[4] Maeve Cummings, Stephen Haag, Donald J. McCubbrey. *Management Information Systems for the Information Age, 5th Edition*. Boston, MA: McGraw-Hill Irwin, 2005.

[5] Anne Sutton. “Computer Error Rocks Alaska's Fund.” *Associated Press*. 20 Mar 2007. http://biz.yahoo.com/ap/070320/lost_data.html?.v=2.

[6] Darrell Dunn. “Many Data Centers Still Have No Risk Management Plan.” *InformationWeek*. 21 Mar 2006. http://www.informationweek.com/showArticle.jhtml;jsessionid=SFFMOHOUSGUJUQSNDLRSKHSCJUNN2JVN?articleID=183701425& queryText=data+center.

[7] “ISO IEC 17799 2005 Information Security Standard Translated into Plain English.” *Praxiom Research Group Limited*. Accessed online 8 Mar 2007. http://www.praxiom.com/iso-17799-2005.htm.

[8]Thierry Chenillot. “Mirroring over long distances on SAN.” *IBM Corporation*. Nov 2005. http://www-03.ibm.com/systems/services/downloads/G565-1451-00.pdf.

[9] “Basic Principles of Fiber Optics.” *Corning*. Accessed online 30 Mar 2007. http://www.corningcablesystems.com/web/college/fibertutorial.nsf/introfro?OpenForm.

Related Research and Recommended Reading

"AT&T 2006 Business Continuity Study."*AT&T Knowledge Ventures*. Accessed online 5 Apr 2006. http://www.att.com/gen/press-room?pid=7922.

"Linear Tape-Open." *Wikipedia*. Accessed online 22 Mar 2007. http://en.wikipedia.org/wiki/Linear_Tape-Open.

"Digital Linear Tape Generations." *Wikipedia*. Accessed online 22 Mar 2007. http://en.wikipedia.org/wiki/Digital_Linear_Tape.

"A Guide for Achieving Successful Information Availability Strategies: Volume IV—Recovery Services." *SunGard Availability Services*. Accessed online 6 Apr 2007. http://www.availability.sungard.com/NR/rdonlyres/70F3076B-F66A-46CF-BECB-18F55FAF3BAE/0/SunGardVol4_RecoveryServices.pdf.

Interviews with these companies:

- FalconStor Software (http://www.falconstor.com). 30 Mar 2007.
- Mendocino Software (http://www.mendocinosoft.com). 2Apr 2007.

Author Bio

Richard Jones

Vice President and Service Director

Emphasis: Disaster recovery and business continuity, server operating systems, high availability and clustering, high performance computing and grids, data center systems and device management

Background: Over 22 years of software engineering, engineering management, project management and product management in the power supply and networking software industry. Responsibilities included Novell's storage, high availability and business continuity technologies including SUSE Linux Enterprise Server and NetWare operating systems.

Primary Distinctions: Top-ranked speaker at Novell BrainShare and Novell partner events.