

# DISASTER RECOVERY

The Journal Dedicated to Business  
Continuity Since 1987

**JOURNAL**

Disaster Recovery Journal

Contents

Summer 2004 - Volume 17, Issue 3

## DATA PROTECTION

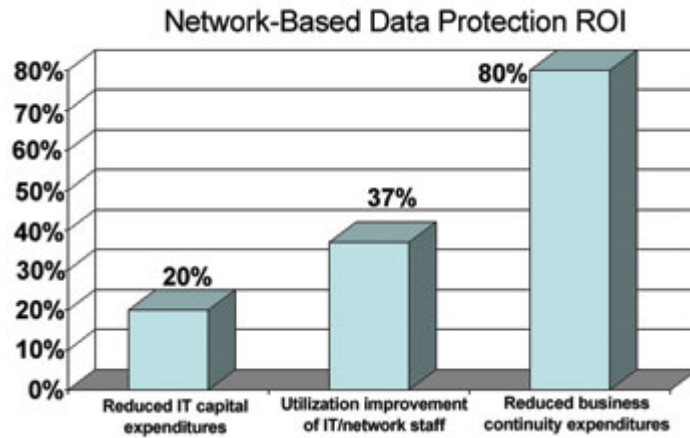
### Mass Exodus: The Movement of Data Off Site

By FRANK BRICK

With the continually rising costs of storage management combined with an onslaught of federal regulations creating increased legal and financial exposure for data loss, executives are challenging IT organizations to find ways to better protect their mission-critical data more cost effectively – and more importantly – off-site. Hence, what started as a tactical response to an increased sense of vulnerability, remote data protection has grown rapidly in popularity as a smart strategic move for businesses of every size.



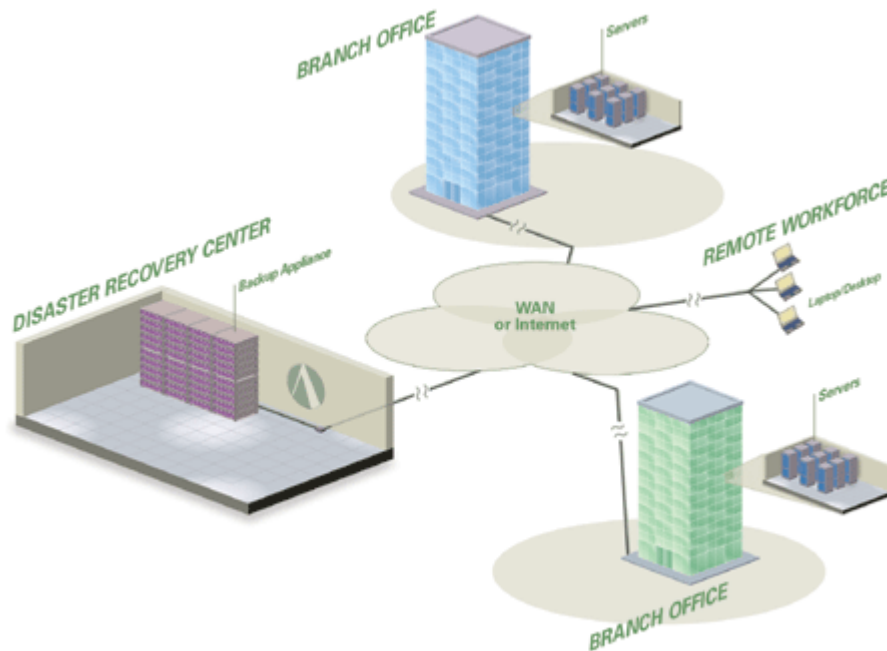
In turn, demand for off-site data protection services has become increasingly desirable as a way to mitigate risk and reduce cost – creating a virtual mass exodus of data. In fact, across companies of all sizes, International Data Corporation (IDC) found that nearly 80 percent plan on implementing business continuity with a redundant data site within the next 12 months.



The challenge is that data considered mission-critical today is very different than it was just a few years ago. Today, more and more data is created, collected, stored and used remotely – that is outside the corporate data center – little of which is regularly backed up. In turn, IDC estimates that as much as 60 percent of corporate data is unprotected on desktops and laptops. It is not surprising then why 64 percent of companies admit their data protection and disaster recovery plans “have significant vulnerabilities” in spite of everything they know about the risks and costs of downtime.

Thinking about moving data off-site but are unsure where to begin? Here are some important questions to ask yourself and your vendors during this process:

- Is remote data protection less expensive than internal solutions?
- Doesn't off-site data protection require expensive dedicated network connections?
- How can you cost-effectively protect data residing outside the corporate data center in dispersed offices?
- How can you cost-effectively protect data on laptops and PCs?
- What will the impact be if backups and restores are made across the company network?
- Is security and control diminished with the data off site?
- What is your recovery time objective and does the service meet this need?



Network-based off-site data protection leverages existing networks to conveniently centralize backups across distributed organizations.

### **The Increasing Efficiency of Network-Based Data Protection**

Historically, most companies have relied on local data protection solutions to backup and restore their data. This centered on the protection of data managed primarily within the corporate data center or “glass house.” Companies would use traditional tape or optical devices to backup and archive data that would then be transported off-site. However, as businesses have become less centralized, more mobile and more geographically dispersed, they realized these local data protection methods were capturing only 40 percent of their business’ applications and data. In turn, the majority of company data that resides outside the glass house was at risk.

Early adopters of outsourced data protection faced several challenges; most notably the requirement for very expensive dedicated high-speed network links that limited its use to data centers and select servers. And in most cases, these services were restricted only to servers running specific operating systems, which still left many branch offices and individual PCs unprotected. That was then. Today, remote data protection services are ushering in a new paradigm for data protection. No longer are these services only for the largest and wealthiest companies. With the help of content addressed storage technologies, on-network backups and restores can occur over existing network connections with increased efficiency by reducing both bandwidth and storage requirements. This means no new investment in networking infrastructure or service levels - just a way to better leverage existing investments.

And since these new remote services can equally backup data from any and all servers, PCs and laptops on the network, this has made it both more convenient and more affordable to protect company-wide data from data center to desktop – across all geographic locations – and to a centralized, secure off-site facility. By centralizing data in an off-site facility, IT organizations can more thoroughly protect company-wide data without requiring additional equipment or resources and without relying on individual users to backup their own data. This not only simplifies backups, but it also speeds restores and rebuilds of PCs and laptops affected by disk crashes, theft and damage.

## **ROI**

Today's outsourced data protection services are generally turnkey solutions that have all of the hardware, software, personnel and 24x7 operations included in the service. Nothing is needed by your business. Even the sophisticated portal used to access and manage the data is web-based and accessible from any networked browser. In turn, businesses can significantly reduce expenditures related to storage provisioning and management. In fact, according to a recent IDC report, companies that do not own their own internal backup infrastructure, but rather rely on an outsourcer to provision business continuity, have reduced business continuity expenditures by more than 80 percent, and lowered IT capital expenditures by more than 20 percent. These savings are fairly immediate. In addition, businesses will also see an increased utilization of personnel as resources once dedicated to storage management are redirected to more revenue producing projects. In fact, the IDC report quoted a utilization improvement of IT/network staff in supporting more employees of nearly 37 percent.

Perhaps most importantly in terms of return on investment in outsourced data protection services, is that revenue loss per incident for those outsourcing their data protection was three-quarters less than those with an internal backup infrastructure. This can be quite significant in the face of grim statistics showing downtime costs for a company average over \$1 million per hour. This means faster recoveries and less disruption to operations, services and production which is critical when you consider that only 6 percent of companies that suffer a catastrophic data loss will survive beyond two years.

## **Simplified Decision-Making**

As remote data protection grows in popularity, companies are increasingly making their storage and network decisions together since remote data protection requires the network as the enabler. Fortunately, one of the inherent strengths of today's network service providers is their internal capabilities in the areas of security, disaster recovery and business continuity. After all, continuous operation is the lifeblood of their business. To this end, network service providers operate some of the most technologically advanced and reliable infrastructures and facilities for business continuity available today. Consequently, storage solutions such as remote backup and restore are

becoming a natural extension of the network service provider's offerings to their customers.

As a result, with an integrated storage and networking solution, not only are businesses enjoying economies of scale with the service, but they are receiving higher levels of security than many internal infrastructures.

### **Summary**

As businesses continue to face rising storage management costs and increasingly stringent regulations for data protection and accessibility, the value of outsourced data protection is going to continue to grow. In turn, the mass exodus of data now underway is only just beginning. It's likely that off-site backups and outsourced data protection services will become the cornerstone of a new generation of business continuity and disaster recovery plans that promise cost-effectiveness and convenience. For companies that have already tapped into services for off-site data protection, it is proving to reduce costs, improve data availability, increase security levels, and reduce restore times.

---

Frank Brick is chairman and CEO of Arsenal Digital Solutions (Cary, NC). Brick can be reached at [frank.brick@arsenaldigital.com](mailto:frank.brick@arsenaldigital.com).

---

*©Copyright 2004 Systems Support Inc. All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of System Support Inc. is prohibited.*