

Recovery Sites: To Insource or Outsource... That Is the Question

By Michael Croy, Forsythe

Disaster recovery hot sites are a hot topic these days, and for good reason. Information systems have grown more important to the success of an organization than ever before. Unless executives carefully evaluate their investments in recovery sites, their organizations can get burned by insufficient access, slow recovery times, and unexpected costs.

IT infrastructures have become more complex, and that has made decisions surrounding IT recovery investments more confusing. Should an organization hire an external provider or establish recovery facilities in-house? Which providers offer the best facilities and service at the best price? What data needs to be recovered? What information needs to be recovered within minutes? What data can be safely and more cost-effectively retrieved within days or weeks? How does the recovery plan ensure that the business continues to function as seamlessly as possible? Does the agreement with the external provider cover all of these issues? What kind of recovery testing is available and when? What's the capability for change management implementation?

The best, most cost-effective answers to those questions require an evaluation of multiple business factors and key insight from both IT and the business organization. Fortunately, reliable and financially viable solutions do exist! The challenge lies in making the best choices for the business.

Proven Value

IT backup and recovery solutions started appearing more than 25 years ago as data assumed a more central role in managing and driving corporate performance.

Over the years, the sector has evolved to the point where recovery providers now offer highly-sophisticated recovery sites. These facilities provide the hardware, software, telecommunications capabilities, and workspace customers need to continue business in the event of a crisis at one or more of their business locations, as well as specialized support services.

The concept of a recovery location, or hot site, was initially based on the notion that most organizations have a relatively similar set of IT infrastructure needs: a large main

frame computer, desktop computers, printers, telecommunications, and network connectivity. In the event of a disaster, organizations would ship their back-up tapes to the hot site, get the operating system up and running, load the back-up information, and continue to run the business.

That basic model has more than demonstrated its value during the past two decades, even as technology and its importance to the organization have changed markedly. The degree to which most organizations rely on their IT infrastructures to drive and manage business has soared, and so has the need for speed when recovery needs strike. System disruptions represent much higher risks today because regulations concerning internal controls and the protection of financial data and customer information have grown much stricter. System outages cost much more than they did 20 years ago when business was less dependent on IT.

As a result, the recovery services sector has developed different types of offerings. Workspace recovery products, for example, replicate certain sections of the business, such as a call center; employees can simply commute to a different location, step into the workspace recovery center, and resume responding to customer calls.

Full-time recovery facilities are now available to organizations 24 hours a day, seven days a week. For example, many financial service organizations today have recovery centers available around the clock. Some of those facilities replicate the firms' trading operations. They might feature 200 work stations, each of which is equipped with four or five computer monitors, the latest and greatest in network connectivity and market data information, and the ability to handle many phone lines at once.

The original IT recovery location model typically featured a shared environment where several organizations paid a fee in exchange for access to the back-up location in the event of a disaster or prolonged business interruption. The success of that model hinged on the assumption that no event would spark a need for all customers to use the recovery facility at the same time.

The Sept. 11, 2001 terrorist attacks on New York City and Washington, DC highlighted some challenges with that model. Recovery facilities in the New York metropolitan area quickly reached capacity in the aftermath of the attacks. Ensuing flight restrictions delayed or prevented organizations from putting their personnel, and perhaps even their critical data, on planes and shipping them to alternate recovery locations in other parts of the country.

Inside or Outside?

Today, the primary investment decision boils down to whether a organization should hire a vendor or handle its recovery needs in-house. Both are viable options. The best business decision depends on a careful analysis of the organization's IT infrastructure and, most important, how its collection of systems and data supports high-level business objectives.

It is also essential to understand the potential benefits of each option:

External Recovery Provider—Internal Recovery

The vendor's knowledge and expertise can be leveraged. Risks related to the use of pooled or shared equipment no longer exist.

Providers typically offer disaster-avoidance services, which may be particularly valuable to small organizations.

Organizations often have better control over their data and better monitoring capabilities.

Most vendors provide top-notch security, power, and telecommunications capabilities. Potential risks associated with the business stability of external provider are not an issue.

Larger vendors often provide logistics assistance when disaster is declared. Change-management activities tend to be more responsive.

Hiring an external recovery site provider usually results in a lower total cost of ownership. There are no disaster-declaration fees (which many external providers assess).

Organizations benefit from minimal impact on internal resources. Organizations can leverage internal assets to achieve cost effectiveness.

Technical issues, such as data security and telecommunications capabilities, mark a crucial consideration—but so do cost factors. For example, providers typically assess a fee equal to one month's contract fee (anywhere from \$10,000 to \$100,000, or more) when a customer declares a disaster. Daily usage fees as much or more than 50% of the monthly fee may be in the contract (depending on the provider). There is also the concern of monthly expenses which will include

subscription fees, testing, software and hardware costs. The best decision depends on a thorough, multi-dimensional analysis of numerous variables.

A balanced evaluation must relate directly to a organization's business needs. It may cost more to establish internal recovery facilities, but the benefits derived from process improvement and customer satisfaction return may outweigh any additional cost. In other cases, the staffing and telecommunications costs associated with setting up internal recovery locations may not justify the access and control benefits that the internal model delivers.

Location, Accessibility and Change

Organizations frequently commit costly mistakes in their selection process, regardless of whether they use an external or internal recovery-center strategy.

Many organizations that opt to house recovery facilities in their own buildings give short shrift to location considerations. For example, an organization headquartered in Ft. Lauderdale, that places its IT and workspace recovery center in a building nearby may be in deep trouble if a flood strikes Ft. Lauderdale. On the other hand, the organization may incur exorbitant expenses if employees need to travel to a recovery center in Phoenix.

Before signing an agreement with an external provider, the business should scrutinize the location and access policies laid out in the contract. Too many organizations neglect contractual language that governs accessibility, test procedures, excess fees (and what triggers them), and the scope of the equipment and services that the agreement includes (or excludes).

The testing process can also cause problems. Large recovery providers have thousands of customers, each of whom needs to test its recovery capabilities on a regular basis. Many customers discover that they cannot conduct those tests with their providers when they need to—when, for example, a significant change in their IT recovery needs occurs. Since most IT environments change regularly, and sometimes radically, it is important that the recovery location keeps pace with those changes throughout the year.

Change management marks a critical piece of an effective recovery site strategy. The recovery facility should mirror changes to the organization's IT and business process infrastructure. To ensure that they do, relationships with outside providers should be closely managed throughout the duration of the agreement.

Some large organizations, particularly those in the financial services industry, boast a team of many disaster recovery professionals headed by a senior vice president. A smaller firm may have only one person assigned to disaster

recovery and business continuity planning. Regardless of a organization's size, the relationship with a recovery site provider should be owned by a senior manager within the executive management team who has deep knowledge of both the IT organization and the business.

Tough Questions

Choosing the most prudent recovery center approach is a complicated process that carries significant risk. Numerous business and technical questions must be answered:

What are the costs associated with using an outside provider vs. building an internal recovery center?

Do recovery time and recovery point objectives require facility exclusivity?

What is the business value of the data in a fiduciary and fiscal context?

What are the drivers for recovering the information?

How critical is the access to and control of the data?

Should testing be controlled by the provider or the business?

What solution ultimately meets the business context of the organization?

Is there a return for the business on the recovery site investment?

There are more questions, all of which must be answered by understanding the ways in which information systems and the data that courses through them affect business performance. If the answers to those questions come easily and accurately, a organization is in an excellent position to make sound decisions about its recovery site strategy. If not, it may be prudent to seek assistance with the complex analysis, given the increasing importance of recovery planning to the business.

Published on CIO.com, December 2, 2004.

Michael Croy is Forsythe's director of business continuity solutions. With more than 20 years of experience, he is responsible for the company's business continuity offerings, including risk analysis, best practice models for continuity of IT infrastructure (storage, server, and network) and disaster recovery planning, strategy, and management.

