MRE Technology SERVICES

WHITE PAPER

HOW TO **PROTECT YOUR DATA FROM DISASTER**

AN EXECUTIVE BRIEF FROM STEPHEN WEBSTER, MRE'S CHIEF TECHNOLOGY OFFICER

As the old adage says, hope for the best but plan for the worst.

This is obviously true in business. Part of an executive's job is to identify the worst things that could happen and determine how to deal with them. This planning should include the protection of your critical systems and data in the event of a disaster. A hurricane or fire that destroys a firm's data could destroy the business itself. That's why disaster planning must include provisions for the safety of a company's critical information.

> This paper will provide a few key things to consider when planning how to protect your data and systems. Start by looking at your data and asking a few critical questions:

HOW MUCH DATA DO YOU HAVE TO PROTECT?

The volume of data varies between types of firms, and this leads to different solutions for ensuring data security. When your data includes primarily accounting and customer order records, a simple offsite backup system should suffice. However, if your data includes significant proprietary information, processes and software tools, you should consider an offsite data center or co-location facility.

Leasing rack space at a respected data center is a viable option given the capital investment required to build your own facility. These facilities are designed to stand up against the worst man and nature can throw at them while still keeping your data constantly available to the right people.

HOW RECENT DO YOU NEED YOUR BACKUP DATA TO BE?

For some businesses, losing a day's or week's worth of data is a small inconvenience and isn't worth the cost of high-frequency backups. For other organizations, losing an hour's worth of data can be catastrophic. In these situations, businesses need a high-frequency backup system, running in the background, that sends data to an offsite location. For companies with a constant flow of new information, a system that backs up data in real time may be a good investment.

How recent the data has to be in order to remain relevant is known as the **Recovery Point Objective (RPO).** It measures how far back in time the data can come from and still be useful. The relevancy requirements will dictate the complexity of the backup system. Knowing your business's RPO can help you make effective planning and budgeting decisions related to your backup systems.

HOW SOON DO YOU NEED TO BE UP AND RUNNING?

Some businesses can be down for 24 hours and lose very little revenue or data. These firms can get by with offsite backups done every 24 hours. Other firms, such as energy traders, can potentially lose millions of dollars if they are down for more than a few minutes. They need to have a simultaneous system running at a second location with near-real-time availability in the event of an outage. How soon a business has to be back online is known as the Recovery Time Objective (RTO).

The RTO numbers play an important role in cost-benefit analysis of backup systems. Ideally, you would prefer to be able to get up and running immediately, but there are cost considerations. If a system with immediate availability has annual costs that exceed the total cost of a backup system that can restore your data in 24 hours, which is the better investment? Take a look at your business processes and consider what RTO makes sense for your firm.

DOES THE DATA HAVE TO BE MAINTAINED IN A SECURE ENVIRONMENT?

While all data must be protected, certain data is far more valuable and requires more protection. For the small enterprise with low-risk data, a good password policy and proper firewalls in both the main operations location and the backup system should provide sufficient protection.

However, oil companies with seismic data worth millions on the international market will need to have a well-designed security infrastructure at the primary business location as wells as a secure data center facility to store its backup information. Such firms will find themselves the target of international intrusion attempts. Both primary and backup systems need to be constantly secure and available. In such situations, purchasing secure space at a data center may be the most efficient solution for your disaster recovery plan.

WHAT ABOUT PEOPLE, PROCESSES & TECHNOLOGY?

Keeping your data safe from disaster also includes assessing the tools needed to do so, the procedures for using those tools and the people who will carry out those procedures. Ask yourself if you have the technology in place to recover after a disaster. Have you thought about where you will set up operations in the event your main location is rendered useless? Do you have the tools to access your backed-up data from this secondary site?

The tools are only effective if there is a plan for using them. This should include a timeline of who will do what at which time.

For example, let's say there is a hurricane in the Gulf of Mexico that is headed for Houston. When does your company begin to switch over to its backup location? What steps need to be taken to secure the computers in the office before the storm hits? Who will perform these steps? If there is a fire in the office, what is the procedure for recovering that data and restarting operations?

(CONTINUED)

(PEOPLE, PROCESSES & TECHNOLOGY CONTINUED)

When it comes to people, you have to ask a completely different set of questions. Has the company identified the right people who will be needed to initiate a disaster recovery? Can the firm provide the necessary resources to people so that they can restart operations? Can the right people access the right data needed to keep the business running?

In addition, it is a good idea to have the capability for employees to access data from remote locations in the event that they cannot get to the backup site. Such offsite accessibility will allow them to keep working and contribute to the restoration of the enterprise regardless of their physical location. It basically allows you to open a branch office in any Starbucks or other WiFi hotspot.

When thinking about people, don't forget about the emotional strain that often accompanies a disaster. Employees will be worried about their jobs, families, homes and possessions. Businesses need to include these concerns when considering how to recover from a disaster. It's easy to say a Houston company will just send employees to a recovery site in Austin where backup data will be available. But will that employee be willing to leave his or her family behind? And if so, how will this impact productivity and quality? It's important to remember personal and practical considerations when assessing your disaster response.

Technology and data are useless without good people to utilize them. From that perspective, here are a few other questions to ask: Is it possible to let employees bring their families along to the backup site? Do your recovery procedures include time to let employees make the personal arrangements necessary to prepare themselves for a predictable disaster (like a hurricane)? What kind of procedures should be in place to ensure that both your people and your data recover from the disaster?

DO STAFF MEMBERS HAVE THE SKILLS REQUIRED?

The process of protection and recovery often requires specialized skills beyond the scope of a qualified IT department. The cost of maintaining such human capital in-house can be prohibitively expensive. If this is the case, it may make sense to hire an outside firm to help establish the infrastructure, systems and procedures necessary to protect your data from disaster.

Large or data-intense firms may also want to have specialists available on a contract basis in the event that calamity should strike. In addition, these specialists can help implement emergency preventative measures, such as having a backup site ready in advance if your main office location is threatened by a hurricane.

Hiring outside experts often gives firms access to a greater degree of expertise at a lower cost than employing full-time resources. This staff acts as an insurance policy for the firm's data.

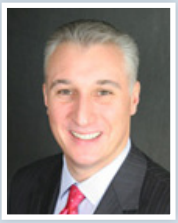
CONCLUSION

An executive should understand that a business relies on its data, and that, sooner or later, your business will have to deal with a disaster.

A detailed analysis of your data and its usage can lead to a disaster recovery plan that minimizes the impact. Addressing the main issues within disaster recovery begins with answers to these questions: How much data do you have? How recent does it have to be? How soon does it need to be available from the backup? How secure do the backups need to be? Do you have the right people, processes and technology in place to maintain the safety of company data and provide the access required to restart the business? Does your staff have the right skills for this job?

If you need help answering any of these questions, MRE Consulting has infrastructure management experts available.

Ask an MRE expert how to keep your data safe.
Contact info@mre-tech.com to start building your disaster recovery program.



ABOUT THE AUTHOR

Stephen Webster is chief technology officer at MRE Consulting, a dynamic professional services firm.