Seven questions your organization should answer about your IT disaster recovery plan

Prepared by:

Mike Simone, *Manager*, McGladrey LLP
816.753.3000, mike.simone@mcgladrey.com

Beth Johnson, *Principal*, McGladrey LLP
816.751.4071, beth.johnson@mcgladrey.com

October 2013

An effective information technology (IT) disaster recovery plan is vital to your company. With the right plan in place, should disaster strike, your IT infrastructure will continue to serve your company and your customers effectively. Without one, a disaster could severely damage or even destroy your company. How prepared is your company to recover from a disaster affecting your IT systems? The answer to that question hinges on the answers to seven other important questions.

Has your company embraced the importance of a disaster recovery plan?

Intellectually, it's easy to make the case for disaster planning, but in reality, it can be difficult to get an organization to devote the time and resources necessary to doing it right. An investment in something you hope you will never use can be a tough sell in this economy.

Leadership is central to an effective plan. You'll need:

- Support from the top—your company's leadership has to buy in and support your IT disaster recovery planning efforts
- Support from across the organization, not just from IT—that means more than just your IT department. You'll need professionals with the appropriate depth of understanding of both your business and IT operations to build an effective plan.
- Support from finance—it may take more than an investment in hours to get the right plan in place. The company may also have to invest in facilities and equipment.

Are you thinking about the business, not just your systems?

While the purpose of an IT disaster recovery plan is to keep IT systems running, or to have them back up as quickly as possible after a disaster, remember that the systems are not an end in themselves—they are there to support your business. Therefore, you will need input from managers of all key business processes to establish the performance parameters that should drive your disaster recovery planning efforts. Follow this outline:

- Inventory all systems and functionalities.
- Work with operational managers to understand the risks and effects associated with each system.
- Ask managers how long they can go without various tools. How long can they be without email and various ERP system components?
- Weight those responses according to the criticality of each item.
- Use those priorities and downtime requirements to establish the parameters of your disaster response effort.

This exercise will set the time frame for your overall response, and will determine the order of which key IT services need to be restored.

Do you know who knows what?

Some disasters, like a flood or fire, are huge. But without planning, a disaster could be something as small as the only person with the knowledge of a particular vital system component leaving your company to take a new job. Develop a list of all the key IT competencies your organization requires and who has them. Cross-train your people to build redundancies in those skills. And monitor that list as new systems come on line and as people leave your company.

Are you taking advantage of virtualization?

Obviously, there are physical elements to any system—servers, routers, terminals, communications infrastructure. But cloud-based and other options make the virtualization of even your core systems not only feasible, but increasingly advisable. Not long ago, the common model was for all the hardware associated with key systems to be located in one or a handful of facilities. A disaster affecting that facility could knock out an entire system, so backup plans focused on a separate physical system in a different location.

Now, companies can mitigate their IT risk by virtualizing their systems. The more virtual those systems become—the more they are distributed—the less vulnerable they are to a disaster affecting any single physical location.

Of course, some systems—telecommunications, for example—still require physical concentrations of equipment, making them vulnerable to physical disasters. So, even if you have effectively virtualized many elements of your key systems, you will still need separate backup and recovery plans for those items. Even if all your core systems remain up and running after a disaster, they won't do much good if your people can't connect to them.

How and where are your systems duplicated?

Whether physical or virtual, duplication is part of an effective IT disaster recovery plan. You need to identify all key system elements, from physical network components to software and data, and have backups in place, ready to take over in the event of disaster. Part of the challenge of disaster planning is budgeting for investment in necessary duplicate components. Disaster planning can be a tough sell on the budgeting front; it only controls risk and doesn't offer any potential increase in revenue. Many companies find it effective to rotate existing equipment to their duplicate facilities, as that equipment is replaced in the course of normal operations, which can reduce the cost of a disaster plan. One caveat: be sure that the older equipment is still up to the job.

Your disaster plan doesn't stop at the door, does it?

The world is increasingly interconnected and interdependent, and your IT operations are no exception. Many financial institutions, for example, rely on outside core processors for key activities, like processing and clearing checks, issuing statements and handling loan payments. In the event of a disaster, a bank would need that relationship to continue to operate effectively. Suppose a bank has virtualized what they can and established a separate, secure backup facility for certain key systems. A disaster strikes and everything works as planned, except they have forgotten to work with their outside core provider to ensure that their backup facility will work with the vendor's system. Because system security is clearly a vital consideration in such a relationship, and because the bank had not coordinated with the outside core processor, the core processor's system does not recognize the Internet Protocol (IP) address of the backup facility, and the bank's operations grind to a halt.

Take these steps:

- Inventory all external IT relationships
- Weigh those external relationships against your key business priorities to understand how they affect operations
- Establish downtime expectations and prioritize the order in which these functions need to be restored
- Coordinate with your external providers to develop recovery plans

Remember, too, that disasters can strike any company—including your vendors. So, checking the adequacy of their recovery plans should be a key part of yours. Are they following disaster planning best practices?

Is everything documented and tested?

Disasters by their very nature are chaotic, so your disaster plan should document everything from what constitutes a disaster to detailed, step-by-step checklists detailing your response.

And having a plan is just a start. Then, you have to make sure it works. Test every element, including the human element. Make sure that systems you are counting on work as advertised. Make sure your people understand their roles. Make sure communications channels are in place—within your company and with your external vendors. Make occasional disaster drills part of your company's routine, so that your people and system will be ready should the time come.

A disaster doesn't have to be disastrous. With the right plan in place, your company can weather the unexpected and continue to effectively serve your customers. Without it, a disaster could close your doors forever.

800.274.3978
www.mcgladrey.com