

Disaster Recovery

How to protect your technology in the event of a disaster

By: Bob Xavier

In the immediate aftermath of September 11, affected technology managers were declaring an emergency. Those companies and organizations that had disaster recovery plans would be operational within hours -- some within seconds. Those that did not have a plan in place probably lost their data.

Disasters can come in many forms -- floods, earthquakes, power outages -- and they can come when you least expect it. The important thing is to be prepared so critical data can be recovered and your organization can become operational as soon as possible. A disaster recovery plan is essential in these cases.

How Critical Is Technology To Your Business?

The first thing to keep in mind is that disaster recovery is a business problem as much as it is a technology problem. The business decision makers need to be involved in establishing the priorities. Which systems are the critical business systems and who supports these systems? Which data is critical and how is it being protected? What are the steps to recover the systems?

For some corporations, integration of their technology plan with their business plan is a necessity. For a nonprofit, the computer systems may or may not be critical to the business. The extent the business relies upon technology will determine the appropriate investment in recovery systems.

Document Systems in Place

The basic steps of developing a disaster recovery plan are the same for any organization. First, define the disaster. We (a Boston-based financial services firm) planned for the complete destruction of our main facility. If that is too overwhelming a disaster to consider, think of what will be the most painful event the organization could survive.

Next, it is important to get an understanding of the systems in place: an inventory of hardware, software, business systems, and all the interactions the systems enable. You have to understand the systems from a whole new perspective--from the point of view of the business. What part of the technology is critical to operations?

Documentation is critical. Make a simple chart of the systems used by the agency: how they are installed, where the installation CDs are located, how they are backed up, and how to get support. Undocumented complexity is the enemy every day, and it is fatal in recovering from a disaster. We started to simplify our network so that recovery would be easier. These simple steps can eliminate the complexity in most organizations:

- Standardize all of the desktops!
- Document the exceptions.
- Store all the data on the servers!
- Document everything!
- No exceptions.

When these rules are followed not only is recovery simpler, but so are everyday operations. We were able to achieve big savings in our support costs and provided better service.

Backing up Your Systems

Once you have defined the disaster and gotten an understanding of your systems, you should then ask yourself:

- Which systems are critical?
- How are the systems backed up?
- How are the systems recovered?

Many organizations have a good backup strategy for at least a portion of their systems, but even if your organization has a rigorous system of backups, without a plan for recovery, you may face insurmountable challenges to recover the systems. Ask what you need to recover the systems, the data, and all of the user documents. Do you have to backup the databases, the documents, and the systems? It can be more complex than it looks, and it's overwhelming in a crises. A good starting point is to ask yourself the following questions:

- Where is our data stored?
- Is all of it backed up regularly?
- How are backups documented?
- Where are the backup tapes stored?

Where Is Support Available?

Finally, it is a good idea to work with a specialized disaster recovery firm for off-site assistance. We negotiated with a recovery firm for emergency server and office space, network and communications links, and emergency personnel. Our mainframes would be restored in Northern New Jersey, our servers in Eastern Massachusetts, and 100 desktops would be delivered within 24 hours. All of these pieces would need to be networked in advance. If an emergency were declared, a whole team of people would spring into action, rebuilding the infrastructure, restoring backup tapes, and, with luck, restoring business operations.

We practiced it to see where the problems were. And then we practiced it again.

The following are links to disaster recovery firms and other resources for more information on disaster preparedness.

Disaster recovery service providers:

- [GE Disaster Recovery](#)

Online tools and resources:

- [Labmice.net's disaster recovery resources](#)
- [Tek Central's disaster recovery resources](#)
- [Disaster Recovery World](#)

Article date: November 27, 2001

Copyright ©2001 CompuMentor. This work is published under a [Creative Commons Attribution-NonCommercial-NoDerivs 2.5 License](#).

