A Few Pointers for Drafting a Disaster-Response System

By Vin D'Amico, Principal
DAMICON, LLC

This article appeared in the *Boston Business Journal* on August 6, 2004

When people hear about disaster-recovery plans, they think about major events. On average, there are about 35 major disasters in the United States every year, according to the Federal Emergency Management Agency. There is a low probability that your business will be severely disrupted by such an event. It's not major disasters that you need to worry about. It's the little things.

Disasters strike every day. Broken water pipes, fires, storms, accidents, power outages, communications failures, equipment problems, virus attacks and terrorist threats. Your company is not the only failure point. If a disaster strikes one of your business partners or suppliers, you may not be able to deliver products or services to your customers.

About 60 percent of businesses that experience a major disaster such as a fire close within two years, according to the Association of Records Managers and Administrators. Further, over 40 percent of companies that experience a disaster never reopen; more than 25 percent of those that do reopen close within two years, states the U.S. Department of Labor.

By being trained and prepared, the impact of any disastrous event can be contained and near normal operations restored in a matter of hours. Disaster survival requires dealing with the following:

- The human factors are the single most important area for surviving a disaster. People are your organization's most valuable asset. Reassuring and educating them in advance of an emergency situation is critical.
- The next area covers major business processes. There may be hundreds of business processes that your organization executes every day. Some are mission critical, some are secondary and the rest are supportive.
- Finally, consider technology areas from computers and software to production machinery, network equipment, printers, telephones, fax machines and copiers. Some or all of this technology may be unavailable during a disaster.

Here are ten simple steps that any business can take to prepare for a disaster scenario.

1. Assemble a cross-functional planning team

This team creates a roadmap for managing disasters including the requirements, impact analysis, and disaster-response process.

2. Select an executive sponsor and a team leader

The executive sponsor clears roadblocks and resolves issues. The team leader is the point person for the planning process.

3. Define roles and choose participants for the response team

The response team oversees execution of the plan after a disaster. Team members coordinate activities and lead recovery efforts. Include representatives from key customers, suppliers and outside service providers on the response team.

4. Catalog business processes

Take inventory of major business processes. The expense of including every business process cannot be justified. Focus on activities that are most critical to the business.

5. Conduct an impact analysis

For each major business process, ask "What would be the impact on the business if this process could not be performed for several days?". Prioritize based on the answers. Use three levels of priority such as critical (recover in 24 hours), important (recover in 72 hours), supportive (recover only if the event is prolonged).

6. Assess recovery options

Consider manual processing options, engaging an outside firm to take over some operations, or establishing a remote, redundant site for mission-critical operations. To protect against a key supplier being hit by a disaster, use a secondary organization for some of your normal workflow.

7. Identify critical systems

Your business is likely to have many desktop, laptop and server computers. There are also firewalls, routers, switches, printers, scanners, fax machines, copiers, telephones, and so forth. Determine which devices are truly critical as measured by your ability to conduct business without them.

8. Examine system administration procedures

Review maintenance activities. Simple disasters can often be avoided by following proper procedures. Also, copies of important paper documents should be stored offsite and/or digitized.

9. Consider redundancy options

Duplicate or mirror critical systems. This can be done on-site and/or off-site depending on the needs of the business. If customers depend upon you for continuous operation or you have contractual obligations for such, then redundancy is essential.

10. Document and test the response plan

Keep the documentation simple and actionable. The document will evolve over time so do not create a large maintenance task. Include network configuration diagrams, company directory, roles and responsibilities for the response team, and specific recovery procedures. At least once a year, conduct a mock disaster followed by a postmortem.

Whenever you undertake a major new business initiative, make disaster-response planning part of the project. What new vulnerabilities does the initiative expose? How will work be done if new systems are unavailable? Be prepared -- don't let a disaster take your business down with it.

Vin D'Amico is Founder and President of DAMICON, LLC, your ADJUNCT CIO™. He is an expert in leveraging open software to drive growth. DAMICON provides Freelance Technical Writing, IT Disaster Response Planning, and Network Security Management services to firms throughout New England. Vin can be reached at vin@damicon.com or by visiting www.damicon.com.