

Managing in a Post-9/11, Post-Katrina World: An Introduction to Disaster-recovery Planning for Technical Communicators

George F. Hayhoe
Mercer University
hayhoe_g@mercer.edu

Abstract

When disaster strikes, helping people survive in the short term is vital but not sufficient. Those touched by a disaster need jobs to pick up their lives again, but jobs do not survive if business hasn't anticipated the possibility of disruption. The companies that survive catastrophic events with minimal negative effect are the ones that have disaster plans to preserve critical data offsite and resume operation at a new location, and that have implemented knowledge management practices allowing them to adjust nimbly to the short- or long-term loss of personnel. Technical communicators must be a part of business recovery planning in the event of natural or human-made disaster because they have critical skills to offer and are a vital part of the business.

Keywords: *disaster recovery planning; technical and professional communication management*

Introduction

Between the terrorist attacks of 2001 and the hurricanes of 2005, the need for disaster planning is hardly news. We've seen literally thousands of lives lost needlessly, homes and businesses destroyed, and futures cast in doubt. Fortunately, those not directly affected by these tragic events have been generous in donating money and time to relieve the suffering of victims. But the story doesn't end there. Those affected by a disaster, whether natural or human-made, need jobs to pick up their lives again, and jobs do not survive if business hasn't anticipated the possibility of such disruption.

To survive catastrophic events with minimal negative effect, companies need disaster plans to preserve critical data offsite, contingency plans to resume operations at a new location if necessary, and knowledge management practices that will

enable them to adjust nimbly to the short- or long-term loss of personnel.

Technical and professional communicators must be a part of business recovery planning in the event of natural or human-made disaster because they have critical skills to offer and are a vital part of the business. Whether you own your own sole-proprietor consultancy or are an employee of a multinational corporation with millions in annual revenue, you need to be involved in planning for disaster recovery.

Data Recovery

These days, computer files are as important a part of most companies' capital as inventory is to a manufacturer. Indeed, in a knowledge economy, data is a company's inventory.

There's an instructive saying in the southern United States: There are two kinds of houses—those that have had termites and those that haven't had them ... yet. The same can be said of data loss: if you haven't experienced it yet, just wait. And because data loss can be caused by hardware or software problems independent of a natural or human-made disaster, a data recovery plan is simply a matter of good business sense.

Data catastrophes vary in scope and scale. You could lose the contents of just a single computer or of a single server. In the case of fire, flood, earthquake, or other large-scale disaster, it's possible that all of the data at an entire location could be lost. You need to plan your backup strategy in such a way as to ensure that you are protected no matter what.

To mitigate loss of data and thus loss of capital, all of the company's data should be backed up on a regular schedule. "All of the company's data" means not only the content of the servers but also

the content of individual computers' storage devices. Even if your software is set up to save by default to the user's network drive and even if your company's employees have been instructed not to save data to a local drive, you should know that people don't always accept the default and don't always follow instructions.

Preparing for a potential data catastrophe requires that the company take three steps.

1. All of the computers in every corporate location, from individual workstations to servers, must be backed up on a regular schedule.

The frequency of the scheduled backups will depend on how critical the data is and how much time you can afford to lose in recreating lost data and how much inconvenience your customers will tolerate if data is lost. Although a week's worth of word-processing and spreadsheet files probably won't require a week to recreate, a week's lost financial transactions could make life very unpleasant for your employees and your customers.

Some individual workstations and even some servers may not need to be backed up as frequently as others. That decision will depend on the criticality of the data that they contain.

2. The backup media must be stored offsite so that they are not destroyed by fire, flood, or other disaster along with the original data.

An elaborate backup plan does you no good at all if the backups are stored at the same location as the original files.

3. You must establish plans for an alternative data center if your original data center is destroyed.

If your enterprise applications run on platforms other than commonly available workstations, you need to have a plan in place for substitute hardware and network accessibility.

Most companies have plans in place for their enterprise data and systems, but they may not have included the data produced by their technical and professional communicators in those plans. You should make certain that all your work files as well as your archival files are backed up and stored in an offsite location in case of disaster. Otherwise, you cannot ensure that they will be available for you and your colleagues to resume work.

Resumption of Operations

What would happen if all or part of your office building were destroyed by fire tonight? What if an earthquake, hurricane, or terrorist attack leveled your corporate headquarters? Does the company have a detailed plan for resuming operations in an alternate location?

Once the immediate aftermath of a disaster has passed, the company can minimize the effects by restarting business as quickly as possible. To do so, it will need office space and equipment to replace what has been lost.

In some locales, there is a surplus of office space available. In such cases, space can generally be obtained quickly and at relatively low cost. But the lack of available office space may pose a problem if the commercial real estate market is tight or if a significant part of your city is destroyed.

Several of the resources listed at the end of this article will help you in planning for this kind of possibility.

A related point is that if your company is located somewhere that is subject to earthquake, hurricane, or other natural disaster, the company should consider encouraging employees to go to a common evacuation destination where the company will relocate temporarily if necessary. Many companies on the U.S. Gulf Coast were unable to resume operations because their employees evacuated from Hurricane Katrina without this type of plan. As a result, the employees were spread over many states, the companies were unable to resume operations, and their employees were left without jobs and incomes.

Knowledge Management

In addition to its data capital, much of your company's wealth is invested in intellectual capital in the form of work processes, policies, and procedures that employees know but that have never been captured. For the company to resume its operations, it needs more than office space, computers, and data. It needs the people and the knowledge required to run the business.

In the case of a significant catastrophe, not all the company's employees will be able to return to work. Some may not survive the event or may be seriously injured. Others will choose not to relocate to wherever the company has decided to resume operations.

The company can do several things so that the employees who are able to return to work can minimize the impact of personnel who do not return and to train new employees if needed.

- Make certain that all work processes for every significant task performed by every employee of the company have been documented.
- Encourage cross-training on work processes so that no process is known and performed by only one employee or only one group.
- Guarantee that all significant corporate policies and procedures have been documented.
- Identify the people responsible for each of these work processes, policies, and procedures.
- Set up a schedule that requires the responsible employees to review documented work processes, policies, and procedures at least once a year; to update any that are not current; and to identify and document any that are new and not yet documented.
- Ensure that copies of the files or paper documents containing all of these work processes, policies, and procedures are stored offsite so that they will survive any natural or human-made disaster.

The Role of the Technical Communicator

In many companies, the knowledge management tasks described above alone will keep a team of technical and professional communicators busy for a long period. But the other planning tasks will also require work that communicators have unique expertise to perform.

We have crucial skills—facilitating cross-functional teams, analyzing audiences and tasks, designing information, testing the usability of paper and electronic documents, and many others—that can help company's bounce back from natural or human-made disasters.

Resources

[1] Disaster Recovery World. The Business Continuity Planning & Disaster Recovery Planning Directory. [Online.] Available: <http://www.disasterrecoveryworld.com/>.

[2] Small Business Association/Institute for Business & Home Safety. Small Business Disaster Planning Guide: A Disaster Planning Toolkit for the Small to Mid-sized Business Owner. [Online.] Available: <http://www.ibhs.org/docs/openforbusiness.pdf>.

[3] U.S. Department of Homeland Security. READYBusiness. [Online.] Available: <http://www.ready.gov/business/index.html>.

[4] U.S. Federal Emergency Management Agency. Emergency Management Guide for Business and Industry. [Online.] Available: <http://www.fema.gov/library/bizindex.shtm>.

About the Author

George Hayhoe is professor of technical communication at Mercer University. He has also taught at East Carolina University, Utah State University, and Virginia Tech. He was formerly project leader for customer information development in the information technology department at the U.S. Department of Energy's Savannah River Site. He is a senior member of IEEE, a member of the IEEE Professional Communication Society administrative committee, and a past president of the Society.