Chapter 10 Disaster Recovery

Chapter Objectives

This chapter will discuss:

- Disaster Recovery is always a late-night phone call away,
- Factors to consider when formulating a Disaster Recovery Plan,
- An organization's business processes as the baseline for a disaster recovery strategy,
- Data's role in conceptualizing disaster recovery, and
- Steps to take in returning the damaged site to normal operations.

10.1 Disaster is Always Just around the Corner

In keeping with Murphy's Law, that whatever can go wrong will go wrong, and at the worst possible time, imagine you're sound asleep the night before the most important day of the organization's week, month, quarter or year. You went to bed a little early in order to be fresh and alert for the long day ahead. But while the day will be stressful, you know that everything is in place.

Suddenly, your peaceful slumber is interrupted by your home phone, cell phone and mobile email device all activating simultaneously. It turns out that the fire alarm system in your building has malfunctioned and deployed the sprinkler system. Water, a threat just as deadly to IT equipment as a human intruder, has destroyed at least some of your infrastructure. Because the deadlines you face cannot be pushed back, you are now forced to spring into action and activate the Disaster Recovery Plan, of which a critical part is the Business Continuity Plan.

Does your organization have a Disaster Recovery Plan? If you don't know if you have a plan, are you in a position of enough seniority that you should know? Rutberg (2005) shares the anecdote of a financial firm who fell victim to a disaster, and noted that the company had recently tested their plan and that it worked almost perfectly, with the exception of the

phone list, which listed some people who were no longer with the company. The four or five critical people were constantly in contact with each other and by the next morning they had approximately one quarter of their staff of fifty-five working at their alternate work site and had not lost access to any of their customers or their data.

10.2 Factors to Be Considered in Formulating a Disaster Recovery Plan

There are several obvious potentialities that must be taken into account when determining how operations would continue in the event of a disruption, but others that may constitute a "disaster" for the organization that would not seem to be so normally. Terrari (2004) wrote that devising a plan consists of asking questions of oneself as to what would be required to keep the organization operating as normal as quickly as possible.

10.2.1 Acts of Nature

Is the organization located in an area that is prone to having major weather events? The staggering impact of Hurricane Katrina on New Orleans, even given the fact that the storm did not hit the city with the force expected, gives all the indication needed to recognize that almost everyone is vulnerable. Earthquakes and floods are two other possibilities. In addition, fires could utterly destroy an organization's physical infrastructure. No place is totally safe from natural disasters, so be certain to account for them in your risk calculations. Does the organization have adequate insurance to recover the damages suffered through an act of nature?

10.2.2 Human Acts

Much more common is a disruption caused by a person's or persons' actions. How much damage could a disgruntled employee accomplish if they were determined to hurt the organization as much as they could? If the IT equipment from your location was stolen, could the organization continue to function effectively? What if you are behind on the rent for your facility and are locked out of it by your landlord? The most famous recent human acts to disrupt operations were those on September 11, 2001, but nothing nearly as dramatic need occur to impact an individual organization.