Basic Rules of Disaster Recovery for any Organization

Disaster Recovery is a large topic. Unfortunately, most people think of this topic in terms of information systems recovery, which is a very important part of the picture, yet there is so much more information that is vital. Our discussion will start with information systems recovery and then in later blogs I will address some of the other factors.

After forty plus years in Information Technology and being involved at various levels of IT and management I defined some basic rules regarding disaster recovery that anyone would be wise to be familiar with.

1. **The capability to back up data in and of itself is useless. Backups of data are often useless or nearly so.**

Backups of data are even dangerous because they can give a false sense of security regarding the ability of an organization to restore itself to operations. How dare I write this? Call the thought police (again!)

Managers seldom keep enough attention on what it takes to restore functionality in the *real* world. Unfortunately, the frustrating realities of this topic are seldom taught in college classes.

What is important is Rule Number Two.

2. **The ability to restore is everything. The entire purpose is restoration of operations after a greater or lesser disaster.**

Thus, a good recovery plan is going to look at everything it takes to recover from a particular disaster scenario and see to it that all possible barriers to successful recovery are imagined, documented, and finally overcome. Here is a *true* example of how it can all go bad:

A high quality US based shoe manufacturer was hit by a fire that destroyed a large part of their factory as well as the server room. When the IT director tried to use the recovery media, he discovered it was literally a hunk of melted plastic. The company lost all records of its customers, its accounts receivable (who owed it how much money), its accounts payable (who and how much it owed) and vast volumes of additional information. From thriving multimillion dollar company to nothing in one evening. One lightning bolt and the ensuing fire.

I investigated and discovered the IT Director reported to the Comptroller of the firm and the Comptroller saw no reason that the IT Director should invest money on off-site backups. Further, the Comptroller refused to spend on the appropriate data safe, insisting that his old safe that had been with the firm forty years was good enough because it was "fireproof". It said so right on the label.

The Comptroller did not understand that the reason his old safe was "fireproof" was that when it got good and hot it started sweating enough vapor inside to prevent the combustion of paper. However, the temperature was far from controlled. Money, contracts, letters from lawyers, etc. were indeed all, "safe", but the vital data the company ran on was a chuck of melted plastic on a shelf in the safe. Neither the IT Director nor the Comptroller continued to receive paychecks from the firm.

Yet the IT staff had been following a rigorous backup schedule...once again, backups can be useless. The good news is that this company had such brand loyalty that customers were actually happy to pay their bills and re-order from their own records. Actually even competitors helped. Nothing beats excellent business practices, providing outstanding value and good customer service.

Stay tuned for more about backup, restore, and other aspects of disaster recovery planning in an upcoming post.

