Group Project 4: Disaster Recovery

Brian Bergstrom

ITCO 251

4/22/17

AIU Online

Michael Pry

When disaster strikes or there is a major security breach, it is always a good idea to have a backup plan. Backing up company data at multiple locations is not only safe, but the quickest way to restore valuable data or downtime. Regular backups to the database should be done regularly. Aside from the actual backups themselves, it is important to create an actual plan of what to do so everyone does not freak out and do further damage. The IT staff needs to study and practice the plan to make sure they are prepared for when tragedy or security breach does happen.

The first thing a company needs to do involving disaster recovery is assembling a disaster recovery team. These must include key points of contact that each may be assigned certain roles to help get the network back up and running. The team should not only have members of the IT department, but all departments up through the highest management personnel (Dean, 2013, p.674).

Documenting everything about the network is also necessary so the team knows where everything is supposed to go and how things are configured when working properly. This includes inventory of all hardware such as desktops, printers, routers, switches, servers, etc. This information is good to have because then things can be easily spotted that need to be fixed is damaged (Department of Homeland Security). Of course, if these devices contain passwords, be sure only authorized IT staff have access to them and not Tom representing the sales team. Tom may not have the router password, but he might have the password to access any software that department uses. Working together as a team is critical in disaster situations because if things are miscommunicated, things can go awry awfully fast.

Three different types of backup methods exist when backing up data. The first is backing up data to optical media such as a USB drive or DVD. Blu-ray DVDs cans store up to 128 GB of data, making them much more useful than just watching movies (Dean, 2013, p.670). Make sure the device is recordable, so data can be placed onto it. This may work for small company data, but for larger companies, one might need another form of backup.

For larger organizations, tape backups may eb appropriate. This involves backing the data up to magnetic tape that uses a tape drive that is connected to the network. Really large environments may have what is called a storage library in a warehouse somewhere, where a physical copy can be retrieved (Dean, 2013, p. 671). This method is easy to implement, but is often very slow compared to other methods.

Most networks these days use network backups which means they back all their data up onto another network (Dean, 2013, p.672). This is done online through cloud storage. This is probably the quickest and safest way of backing things up because if all the hardware is gone from one location, it can easily be backed up and recovered from anywhere. This is the backup implementation that is best to use for our company because we have locations all over the world. Having the same backups as other parts of the world is critical as then the data is the most up to date no matter where employees may travel.

The next decision in the plan is to decide how much of the data needs to be backed up. An archive bit is a tool that helps determine just that. The bit is turned on when a file is created, telling the system the file needs to be archived. There are three types of backups that can be done: full backup, incremental backup, or differential backup. Full backups backup all data regardless of changes. They then switch the archive bit to off after it is done. In incremental backup, it only backs up the changed files since the last incremental or full backup meaning those files that still have the archive bit checked. This makes it quicker to backup so a full backup is not needed, taking less valuable time. Differential backups are similar except they do not uncheck the archive bits after the backup is complete (Dean, 2013, p.672). Each backup will be different for each situation. However, developing backup rotation scheme can be useful so all types of data can get backed up on a regular basis, leaving backups to practically run themselves at the time of recovery.