Running Head: DISASTER RECOVERY

Documenting the Data Center: Disaster Recovery

Jered McClure

Walden University

Documenting the Data Center: Disaster Recovery

During data center constructions, a key point to have considered and to maintain post construction is disaster recovery (DR) procedures and documentation. These physical and digital documents will ensure that PPI survive anything that may bring their operations to a halt. Whether this be environmental, manmade, or political, documentation and preparation are keys to corporate governance in the face of overwhelming odds.

Specific documentation to keep on hand are: emergency contacts, evacuation plans, restart procedures, and secondary DR locations. Emergency contacts are those people who have the most knowledge about the data center and how to get it back up and running as soon as possible. Evacuation plans are details on where to take sensitive/vital software/hardware if disaster strikes at a given location. In the event that a disaster is recoverable in the immediate time frame of the event, restart procedures for the data center will assist in getting the organization back to operation. If recovery is not immediately an option, a secondary operations location for the data center should be made available and a planned extraction to this location recorded in the procedures.

The DR policies and procedures should be reviewed and updated on a bi-annual basis. It is likely that major changes will not be required. However, recursive review will ensure that they do not become outdated or useless. While disaster may never happen, ensuring the organization is prepared for such an event will make all the difference in organizational capital adequacy.

Responsibility for these documents should be a joint effort between the data center manager and the organizational Risk department. The data center manager should be in charge of the planning and technical aspects, while the Risk department is in charge of compliance and organizational governance. By having the responsibility split between these two entities, the chances of the policies and procedures going stagnant is also lessened.

Documentation maintenance plans should be monitored and maintained through a core risk system. E.g. a scheduled compliance task should be sent out to the manager of Risk and the data center manager to review and update the DR policy and procedures on a bi-annual basis. If changes are made in the midterm of these schedules, DR policy and procedures can be updated. However, due to DR being a rare occurrence, a bi-annual will assure the most organizational protection with the least amount of operational interference.

DR can consist of one of two options: 1) a fully functional hardware equipped secondary location in a 2N capacity; 2) a virtualized 3rd party data center location where all systems are backed up and operations can resume while the organizational data center is recovered. The plus side of the 2N solution is that the organization has all hardware and software under corporate control and governance. However, 2N can be cost prohibitive as it requires a complete second solution be built. The pro of a virtualized 3rd party is that all equipment and hardware can be kept offline and off-lease until such time as DR is required. The downside to this is that if any dispute occurs with the leasing organization, governance may be lost.

Overall, DR is a requirement for the data center that is as important, if not more so, than the data center itself. In the event of catastrophe, a solid plan and awareness on how to execute said plan are what separate profitable organizations from those who disappear into the ether. Moreover, these policies and procedures should be kept up to date, and reviewed on a regular basis.

Reference

Alger, D. (2005). *Build the Best Data Center Facility for Your Business.* Indianapolis: Cisco Press.

Alger, D. (2010). *Grow a Greener Data Center.* Indianapolis: Cisco Press.