Disaster Planning – Documentation and Buy-In

This is the second of a three-part series regarding Disaster Planning. In part two, we will discuss documentation of the plan and buy-in from management and colleagues.

Disaster planning does not just involve having a backup plan for the data in your servers. It is the overarching document that guides your employees and partners in restoring functionality to your organization. Since technology and systems are constantly being updated or changed, this plan should be considered a "living document." Changes to systems, teams and architecture must be accounted for in your disaster recovery plan as they happen. This information must also be available to everyone responsible for any part of the recovery process.

When key IT personnel leave your organization, whatever information they have not documented often goes with them. Undocumented information about systems, procedures or necessary business information can be characterized as "Tribal Lore." When key employees leave, having solid documentation about the systems and business processes enables you to seamlessly onboard someone else in that position. In the case of Disaster Recovery, where time is a crucial factor, you do not have the luxury of time.

It is much harder to recreate any "Tribal Lore" that is required to get mission critical systems and data to a point of viable recovery. It is imperative that clear, easy-to-access documentation of the steps, operations and responsibilities of each person be updated regularly and maintained.

A disaster recovery plan usually has the following sections:

1. An introduction gives the objective of a disaster recovery plan and indicates who has approved the plan and links to other important documents.
2. The roles and responsibilities section shows the responsibilities of team members, their contacts and their limits of authority in case of a disaster.
3. An incident response plan is a step-by-step guide of recommended procedures that are required to recognize and respond to an incident and diminish the negative effects of possible disasters. It is one of the most important parts of a Disaster Recovery Plan.
4. Plan activation identifies the cases when a disaster recovery plan should be launched and the procedures of informing disaster recovery members to start participating in the appropriate actions.
5. Document history shows when the document was revised and who performed the approvement of revision.
6. Procedures show what actions should be performed to bring work back to normal. The more detailed the description of the procedure is, the more successful the disaster

recovery plan will be. This section is extremely important in terms of reliability and stable work and should be presented clearly.
7. Appendixes show system inventories, application inventories, network asset inventories, contracts and service-level agreements, supplier contact data or any other documentation.

After a disaster recovery plan is written, staff members should be trained to follow the procedures described in the plan. Top leadership must support and be involved in the development of the disaster recovery planning process. Management must assign an individual to coordinate the development of the Disaster Recovery Plan and ensure its effectiveness to enable an organization to recover in the event of a disaster. A planning committee should be used to oversee the development and implementation of the plan. This planning committee should include representatives from all functional areas of the organization. Key committee members should include the Operations Manager and an IT Representative. The committee should also include representatives from key areas of the organization such as information systems development, operations, communications and key business units.

In Part-Three, we will discuss Testing and Maintenance of the plan.

The Texas Water Conservation Risk Management Fund's Cyber Risk Control Program provides "Table-Top" exercises for members to test their plans against real life scenarios. It is a valuable service to help identify gaps and areas of improvement of individual member plans.

For information on the Texas Water Conservation Risk Management Fund Cyber Risk Control Program, including IT Risk Assessments, policies, procedures and best practices visit: www.twcarmf.org/cyber-security or contact Lee Cain at lee.cain@sedgwick.com.