Data Security

10 Questions a CEO should ask the IT Director About Disaster Recovery

Most companies have a Disaster Recovery (DR) plan in place. But many do not update it as often as they should, and few test as comprehensively as they ought to. That means that if a problem does occur, your company faces slow recovery, lost revenue and damaged customer relations.

Think it won't happen to your company? Consider this. In a global disaster recovery preparedness survey, Forrester Research and Disaster Recovery Journal found that more than 25 percent of the respondents experienced a disaster situation in the past five years! That's one in every four companies.

What can you do? Ask your IT Director these 10 questions and make sure you get reliable and confident replies to each. If in doubt, engage a DR expert for a Disaster Recovery review.

1. *What are our objectives this year for exercising a disaster recovery plan?*

   Disaster recovery exercises need specific objectives and goals. Clearly, one of the important goals in disaster recovery is to recover all components. But how quickly should they be restored? In what order should they be restored? You may need component X to be recovered before component Y, which depends on component X. What then? Objectives can also be training-related, such that certain employees are assigned successfully complete all the steps for recovering component Y.

2. *Who are the business stakeholders involved in the exercise?*

   The business stakeholders' responsibility is to validate the success of an exercise. They must be involved from the beginning of the exercise until all critical components and business processes are properly restored. This confirms that the business stakeholders know what should happen when a disaster recovery plan is enforced.

3. *Do we rotate staff responsibilities?*

   Rotating less knowledgeable employees in the exercise assures the validity of the training and provides cross-training. It also increases the company's chances of finding hidden risks when for example, a systems administrator executes steps done by the database administrator. Furthermore, you don't want the person who writes the plan to execute the test.

4. *What are the risk scenarios for these exercises?*

   Exercises need to be more specific than telling the response team to assume the data center has been flooded. Different disasters drive different actions. And developing specific scenarios provides the staff with realistic situations to experience. The more they practice, the more confident they'll be and the safer your company.

5. *Do we work with the business continuity team to run joint exercises?*

   In larger companies, disaster recovery and business continuity teams are separate. If this is the case in your business, both teams need to run exercises simultaneously at least once a year. This identifies communication loopholes before, during and after the exercise along with any problems that may occur with both teams doing their jobs. It shouldn't be a siloed effort. To succeed, companies need to take a holistic approach.

6. *Do we change exercise types and include non-technical exercises, such as walk-throughs and tabletop?*

   Companies often cite communication issues and employee role-confusion as the leading cause of a failed exercise. Doing non-technical exercises uncovers issues with internal and external communications, relocation planning and execution, decision-making and logistics. Also, while walk-throughs and tabletop exercises don't check the technical capabilities of a failover, they help with readiness, understanding and training.

7. *Do we exercise all IT infrastructures simultaneously at least once a year?*

   With staff turnover and changing system assets, a lot can happen in a year. Running full exercises at least once per year — some companies do full tests four times per year — keeps current staff up to speed on the processes. Prepared companies also run component tests between full tests. The frequency for these depends on system criticality and environment changes.

8. *Do we have the right members on the core disaster recovery response team?*

   An effective core response team consists of people who can handle extreme pressure, long hours and sleep deprivation. These individuals know how to remain calm during exercises and other high-stress situations.

9. *What are some mistakes that have occurred during exercises and how have we learned from them?*

   The exercises do more than prepare staff for a disaster. They're also an opportunity to find problems and update the disaster recovery plan with best practices based on the lessons learned. If the staff doesn't find mistakes, then the exercises may be too general or not thorough enough.

10. *Have you reported disaster recovery exercise results to stakeholders?*

    Executives and business stakeholders want to know how prepared the company is for disaster recovery and whether they're getting a return on investment. Reporting what went well and what needs improving adds visibility to the disaster recovery preparedness program and lends credibility to the CEO and your IT team. It says that you're abreast of and in sync with best practices as you should be.

ABOUT QUEST

A trusted technology management company delivering successful solutions for clients ranging from the Fortune 50 to Fortune 5000 small and medium-sized businesses, Quest offers a portfolio of professional, cloud, and managed services either on-site or from its secure network of global service delivery centers. Quest is ranked #9 on the Global Managed Services Cloud Providers Top 100 by MSPmentor, is ranked among the top 500 technology firms by VARBusiness, is among CRN's top 250 Tech Elite, and is included in CRN's designation of Cloud Elite.

Visit us at www.questsys.com.