8.9 Test Specific Recovery Procedures

Your plan may look good on paper, but how viable is it? The last thing you want after a disaster strikes is a backup system failure. A common problem is that companies make backup copies of software and data but then fail to make sure that they work. What good is a plan if you fail to test it? Test your planned recovery procedures to find out if they will work the way you expect them to work.

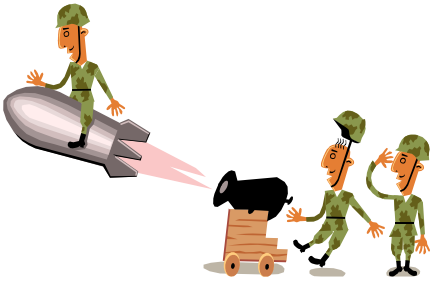
Consider the following when establishing test recovery procedures to validate your network protection plan:

A. Perform regular and periodic testing and drills. Make testing an essential part of your control systems – establish a schedule for periodic drills, exercises, and testing.

B. Test and retest backup systems. Make sure your backup systems will work when needed by testing them often. In particular, perform rigorous testing of backup tapes, backup power supply devices, redundant network file servers and connecting equipment, fire protection systems, offsite backup systems, and any other backup systems that are essential to restarting mission-critical business functions.

C. Walk through disaster scenarios and recovery procedures. Hold formal meetings to review disaster scenarios and make clear individual responsibilities for performing recovery procedures.

D. Simulate major disaster situations. Make sure the company practices for major disasters. Perform a full test reflecting a situation in which you're denied access to your facilities. Do a test to simulate a major disaster at least annually.



E. Include users in testing. Include computer users on the test teams and encourage comments. If the plan designates, actually send team members to the recovery site and evaluate the test results. Although such testing may be costly and time consuming, it could uncover weaknesses in your plan that otherwise might be overlooked.

F. Include auditors in testing. Arrange for internal and/or external auditors to attend tests. Their reports with test results to top management or the board audit committee can instill confidence and/or initiate the allocation of additional resources to install improved backup systems.

G. Let computer experts critique your plan and testing. Work with computer experts to develop test criteria and relevant scenarios. Their knowledge and contribution to the development of a computer network protection plan could ultimately save the business.